PRIVACY AND HEALTH INFORMATION

A Joint Report From

Consumers' Association of Canada
Association des consommateurs du Canada

PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DEFENSE DE L'INTERET PUBLIC

May 2002

This study was made possible through funding under the Contributions Program for Non-Profit Consumer and Voluntary Organizations administered by the Office of Consumers Affairs of Industry Canada

This study was produced by

CAC - Consumers' Association of Canada
267 O'Connor Street, Suite 404, Ottawa,
Ontario, Canada K2P 1V3
Phone: (613) 238-2533; Fax: (613) 563-2254
E-mail: ***info@consumer.ca*** ***www.consumer.ca***

PIAC - Public Interest Advocacy Centre
ONE Nicholas Street, Suite 1204, Ottawa, Ontario, Canada K1N 7B7
Tel: (613) 562-4002. Fax: (613) 562-0007.
e-mail: piac@piac.ca . http://www.piac.ca

TAG - The Action Group for (CAC)
112 Kent. St., Suite 790, Ottawa, Ontario, K1P 5P2
Cell: (613) 298-9834 Fax: (613) 567-7790
nchamber@ccs.carleton.ca

For information on the participating organizations and details on the authors of the study please see Appendix D of the report.

PRIVACY AND HEALTH INFORMATION

TABLE OF CONTENTS

Executive Summary

The enactment of recent federal and provincial level legislation aimed at ensuring the privacy of personal information has engendered a heated debate within the health sector about what privacy means in this context and how personal privacy can be ensured while taking into consideration the many necessary secondary uses of health information. Among these, for instance, medical research, health system audits and evaluation, and epidemiology to name a few. The polarization in this debate, between good health care and research on the one hand and privacy on the other is not beneficial to consumers, who should have a right to both.

To better understand the consumer perspective in this debate and to provide a context within which to understand that view, a three-tiered research project was undertaken by the Consumers' Association of Canada and the Public Interest Advocacy Centre. Consumers themselves were approached and asked their views on some of the key issues in the debate, both by means of a cross-Canada written survey and five regional focus groups, in Alberta, Manitoba and the national Capital region (in both English and French). Results from this research were examined in the light of a review of health sector stakeholder groups' positions and a comparison of relevant legislative initiatives from four provinces and the federal government.

Among the stakeholders groups, little consensus was evident with regard to the particulars, but greater agreement on some general premises, such as the need for informed consent. One of the strongest differences was between groups interested in research and other groups. Researchers (and those who support them) believe certain research purposes require the collection, use and disclosure of personal health information without consent, given that obtaining consent would be impracticable and might jeopardize the research results if it resulted in incomplete information sources. Others groups object that the loss of control inherent in allowing research without consent was aberrant to the notion of informational privacy.

While the sample of consumers who participated in discussions on this issue and/or completed the written survey was not large (approximately 90), there was considerable agreement on the fact that privacy is an important issue for Canadian consumers, but that it is an issue that is not well understood by most. On the issue of consent, consumers believed that: consent should be made as simple as possible and that consent for treatment and for use of personal health information beyond that treatment should be obtained separately. Consumers, on the whole, were not sure how their personal information is currently protected, nor exactly who has access to their information. Research was viewed as a worthy endeavour and almost all those surveyed would want their personal health information used for research, but many consumers wish the

right to refuse consent if they object ethically to the research or find it non-compelling. Consumers were also very uncertain where to turn in case of a breach of confidentiality.

A review of extant and proposed legislation on privacy at the provincial and federal level showed that the different jurisdictions have developed substantially different approaches to the issues involved in the consent to collect, use and disclose personal health information. What constitutes informed consent, and where is it required were two issues that were dealt with variously across legislation reviewed. Another approach differing from province to province was with regard to the rules surrounding the provision of information to the ministries responsible for health care. Provisions in the legislation regarding research using personal health information without consent varied also. Each jurisdiction (except the federal) authorized some form of research ethics board to decide what research proposals should be allowed but the oversight, constitution and accountability of these bodies varied greatly.

From these three discrete research foci, several gaps were identified and recommendations for action proposed. Consumers are clearly not aware of current legislation nor even standard practices when it comes to access, use and disclosure of personal health information. A concerted effort is required to inform the public of their rights and to encourage them to become more aware of the implications of lapses in privacy protection. At the same time, many of the terms used in this debate require clarification not only for consumers but among stakeholders and in regulations stemming from the legislation. 'What is entailed in informed consent?' and 'When is implied consent appropriate?' are two questions that stand out. In the context of the former, this report recommends consent for treatment should be separate from consent to use personal health information for secondary purposes, so that the implications of the latter can be spelled out. In the case of implied consent, it recommends a reconciliation of views between stakeholders and legislators, on the one hand, for whom implicit consent plays a central role, and consumers on the other, who, for the most part do not see the term as particularly meaningful.

Given consumers' desire and legislative support for ongoing control of personal information, some sort of tracking system that allows different layers of consent for different uses of the information will be required. This should not be difficult given ever improving data management techniques. What must be ensured, however, is that consumers can access their record periodically and change their consent "profile" as new personal information is added to their file. Such a system should also permit the tracking of who has accessed specific personal health information, so that whoever disseminates that information can be held accountable. Consumers should also be made aware of the rights they have to access their own information and incorporate changes if the information is found to be inaccurate. While all the legislation reviewed made provisions for individual's access and correction, within certain guidelines, it seemed clear from consumer experiences that some health care providers were unaware of this consumer right. For that reason, health care providers may need to be better educated about these rights as well.

Overall, the researchers found more consensus and overlap among the three research areas than disagreement. In most cases what is required is greater clarification and transparency of procedures as well as a much improved system of information promulgation. None of the issues identified appear to be insurmountable, but they will require effort, co-operation, compromise and a will to succeed, if progress is to be made.

Sommaire

La récente promulgation des dispositions législatives fédérales et provinciales sur la protection des renseignements personnels a suscité un grand débat au sein du secteur de la santé sur ce qu'on entend par protection de la vie privée dans ce contexte et sur la façon d'assurer le respect de la vie privée tout en tenant compte de la nécessité des nombreuses utilisations secondaires des renseignements en matière de santé. Parmi celles-ci on compte, par exemple, la recherche médicale, les vérifications et les évaluations des systèmes de santé, et l'épidémiologie, pour n'en citer que quelques-unes. L'opposition croissante dans ce débat entre les soins et la recherche en santé d'une part et la protection des renseignements personnels de l'autre nuit aux consommateurs, eux qui ont droit à ces deux aspects.

Afin de mieux comprendre la perspective du consommateur dans ce débat et d'établir un contexte dans lequel celle-ci se place, l'Association des consommateurs du Canada et le Centre pour la défense de l'intérêt public (PIAC) ont entrepris un projet de recherche sur trois volets. On s'est adressé à des consommateurs pour leur demander leur opinion sur certaines des questions-clés de ce débat au moyen d'un sondage par écrit à l'échelle du Canada et de cinq groupes de consultation régionale en Alberta, au Manitoba et dans la Région de la capitale nationale (en anglais et en français). Les résultats de cette recherche ont été examinés sous l'angle d'un bilan des positions prises par les groupes d'intervenants dans le secteur de la santé et d'une comparaison des dispositions législatives de quatre provinces et du gouvernement fédéral.

Chez les intervenants il y a eu peu d'opinions communes sur les détails, mais un plus grand accord sur certains principes généraux, tels que la nécessité du consentement éclairé. L'une des différences les plus marquées s'est manifestée entre les groupes intéressés par la recherche et les autres groupes. Les chercheurs (et leurs partisans) estiment que certains buts de recherche nécessitent la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé sans consentement, étant donné qu'il serait impraticable d'obtenir le consentement et que cela pourrait fausser les résultats de la recherche en donnant lieu à des sources d'information incomplète. D'autres groupes ont objecté que la perte de contrôle rattachée à la permission de mener des recherches sans consentement était inconciliable avec la notion de protection de l'information.

Bien que l'échantillon des consommateurs qui ont participé aux discussions sur ce sujet ou qui ont complété le sondage par écrit ne soit pas important (environ 90 personnes), un accord considérable est ressorti sur le fait que le respect de la vie privée est une question importante pour les consommateurs canadiens, mais qu'il s'agit là d'une question que la plupart ne comprennent pas bien. Sur la question du consentement, les consommateurs étaient d'avis que le consentement devrait être simplifié autant que possible, et que le consentement au traitement et le consentement à l'utilisation de renseignements personnels

sur la santé en dehors du traitement devraient être obtenus séparément. Dans l'ensemble, les consommateurs ne savaient pas très bien comment leurs renseignements personnels sont utilisés actuellement, ni exactement qui a accès à ces informations. Selon eux la recherche est une activité louable et presque tous ceux qui ont participé au sondage voulaient bien qu'on utilise leurs renseignements personnels sur la santé pour mener des recherches, mais plusieurs consommateurs souhaitaient pouvoir refuser leur consentement s'ils s'opposent moralement à la recherche en question ou s'ils n'y voient pas d'intérêt. Par ailleurs, les consommateurs ignoraient quelles ressources étaient à leur disposition en cas de manquement à la confidentialité.

Un examen des dispositions législatives déjà en place et des projets de loi sur la protection des renseignements personnels aux niveaux fédéral et provincial a démontré que les divers gouvernements ont élaboré des approches considérablement différentes pour traiter les questions concernant le consentement à la collecte, à l'utilisation et à la divulgation des renseignements personnels sur la santé. Ce que l'on entend par « consentement éclairé » et quand celui-ci est nécessaire sont deux questions traitées diversement dans les lois examinées. Une autre approche variant d'une province à l'autre concerne les règles qui gouvernent la communication de renseignements aux ministères responsables des soins de santé. Les dispositions des lois régissant la recherche basée sur des renseignements personnels sur la santé utilisés sans consentement varient également. Chaque juridiction (à l'exception du gouvernement fédéral) autorise à une forme de comité d'éthique de la recherche de décider quelles propositions de recherche sont permises, mais la surveillance, la composition et la responsabilité de ces organismes varie beaucoup.

À partir de ces trois objectifs de recherche distincts, plusieurs lacunes ont été repérées et des recommandations de mesures à prendre ont été proposées. Les consommateurs ne sont clairement pas au courant des dispositions législatives actuelles ni même des pratiques courantes concernant l'accès, l'utilisation et la divulgation de renseignements personnels sur la santé. Il faut donc un effort concerté pour informer le public sur ses droits et l'encourager à mieux comprendre les implications associées aux manquements à la protection de la vie privée. En même temps, il est nécessaire d'éclaircir plusieurs des termes employés dans ce débat non seulement pour les consommateurs mais également chez les intervenants et dans les réglementations tirées de la loi. « En quoi consiste le consentement éclairé? » et « Quand le consentement implicite convient-il? » sont deux questions saillantes. Dans le cadre de la première question, ce rapport recommande que le consentement au traitement soit séparé du consentement à l'utilisation des renseignements personnels sur la santé pour des buts secondaires, afin que les implications de cette utilisation soient expressément formulées. Pour ce qui est du consentement implicite, il recommande de réconcilier d'une part les opinions des intervenants et des législateurs, pour qui le consentement implicite joue un rôle primordial, et d'autre part celles des consommateurs, pour qui en général le terme n'a pas particulièrement de sens.

Étant donné que les consommateurs souhaitent un contrôle continu des renseignements personnels et compte tenu de l'appui législatif sur cette question, il faudra un système de suivi de quelque sorte qui permette d'établir différents niveaux de consentement pour différentes utilisations des renseignements. Cela ne devrait pas être difficile à réaliser avec les techniques de gestion des données qui ne cessent de s'améliorer. Il faut cependant s'assurer que les consommateurs puissent accéder à leur dossier périodiquement pour modifier leur « profil » de consentement au fur et à mesure que de nouveaux renseignements personnels y sont ajoutés. Un tel système devrait aussi permettre d'identifier qui a accédé à des renseignements personnels spécifiques pour que quiconque les divulgue puisse être tenu responsable. Les consommateurs devraient aussi savoir qu'ils ont le droit d'accéder à leurs propres renseignements et de les rectifier s'ils sont inexacts. Bien que toutes les lois examinées prévoient des dispositions qui permettent à une personne d'avoir accès à ses renseignements personnels et de les corriger dans certaines limites, il semblerait d'après les expériences des consommateurs que certains fournisseurs de soins de santé n'étaient pas au courant de ce droit du consommateur. C'est pourquoi il pourrait s'avérer nécessaire de mieux sensibiliser également les fournisseurs de soins de santé sur ces droits.

Dans l'ensemble, les chercheurs ont trouvé plus de consensus et de recoupement que de désaccord dans les trois cadres de recherche. Dans la plupart des cas, ce qu'il faut c'est davantage de clarification et de transparence dans les procédures ainsi qu'une nette amélioration du système de diffusion de l'information. Aucun des problèmes identifiés ne semble insurmontable, mais il faudra du travail, de la coopération, du compromis et la volonté de réussir pour faire des progrès.

1 Introduction

The debate over the privacy of personal health information has been characterized as one of competing values. Privacy is juxtaposed with the provision of health care, because numerous sources tell us if we are to continue to conduct important, life-saving research, manage our health care system and increase its cost efficiencies, we need to make compromises in the area of privacy. This report approaches the debate from a somewhat different perspective. It seeks to clarify what aspects of continued good health care are compatible with good privacy protection. However, it is recognized that competing values are a key part of the context of this report.

Competing values have become much more polarized as the ability to share information has enhanced the possibilities of using personal health information for purposes other than the direct treatment of the individuals whose health information is in question.

1.1 Purpose and overview of the study

The ability to share information has grown with technology, and individuals can no longer be confident that the health information they give to their health care providers, employers or insurance companies will stay in neat files, accessed only by trusted staff members and used only to provide care or payment. This report attempts to ascertain how consumers view the existing system, what their experiences and fears are about the system, and how the system might better protect privacy. Consumers' needs are compared to the positions taken by various other stakeholders, and the statutory developments in the area. These privacy statutes are the reaction of some jurisdictions to the development of databases, data matching and the looming prospect of security risks such as "hacking". The debate around how and what protections should be applied to personal health information highlights the need for research on what the consumer perspective on the key issues might be.

There are three reasons this report was undertaken, and commensurately, three areas of investigation.

1) Health information is being increasingly shared, and more and more parties are interested in having access to data for legitimate needs that will benefit society, and/or for needs influenced by the prospect of financial gain. This report attempts to investigate consumers' awareness of these changes, and consumers' experiences and perceptions of the state of health privacy.

2) There is a heightened awareness throughout the health community that questions regarding health privacy issues need to be answered and the issues resolved. For example, on the issue of consent, the experts representing the various stakeholders who deliver, receive, or pay for health care, as well as those who conduct research, agree that clarity is needed. Agreement is needed in defining key terms, in setting out practical ways to demonstrate

informed consent, in determining what exceptional circumstances should allow for collection, use and disclosure of information without consent, as well as clarifying how existing statutes ought to be interpreted. However, stakeholder groups cannot agree on the answers and practical solutions. This report reviews their positions, together with legislative initiatives, and compare them to the views expressed by consumers.

3) The legislative response to privacy concerns and the proliferation of electronic forms of personal information has been varied. Because of this disagreement regarding how to handle health privacy concerns in a regulatory fashion, a review of recent relevant legislation is included, in order to review the approaches available. It serves as a background for the consumer research, informing the choice of issues investigated in the focus groups and surveys.

The report first explores the recent history of health privacy, by examining the positions of stakeholder groups through an analysis of their position papers. The results of primary research that was conducted to understand the consumer perspective are then explained, followed by a review of statutory responses that compare five recently enacted or proposed health privacy Acts. The three perspectives are then compared to identify the gaps between consumers' positions on the debate, other stakeholder positions on the debate, and treatment of the issues by the government as demonstrated in statutes. Recommendations and conclusions follow.

1.2 Assumptions

It is important to note that the authors of this report, the Consumers' Association of Canada (CAC) and the Public Interest Advocacy Centre (PIAC) are not independent observers of the health privacy debate. Members of both organizations have been instrumental in contributing to the development of codes and legislation regarding privacy, in general, as well as in the area of personal health information (more information about CAC and PIAC follows, in section 1.7). In part because the CAC and PIAC have been so involved in the debate, The Action Group (TAG), an impartial consulting firm, was contracted to conduct the primary research on consumer opinions.

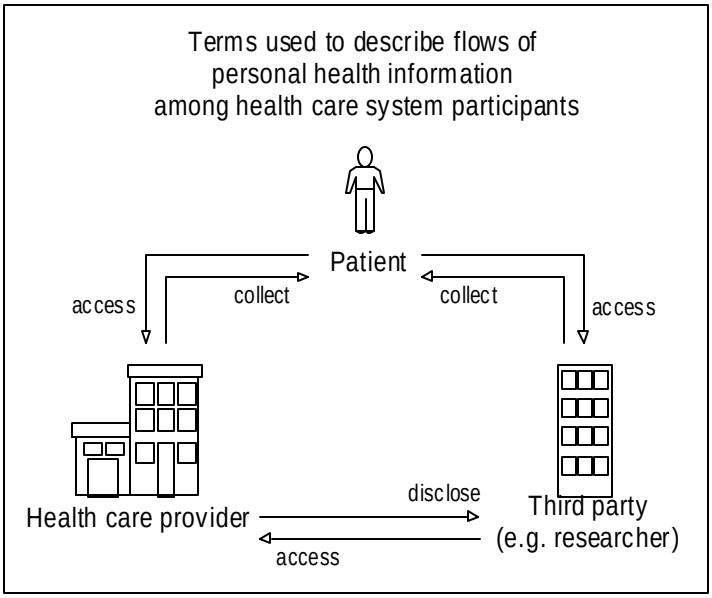
1.3 What is health privacy?

The working definition adopted in this report is that health information privacy is control over information relating to one's health. Understandably, a great deal of information can be considered in this category. For example, it includes the information taken down by a physician, communicated to a specialist, recorded in psychotherapy notes, included in laboratory results, reviewed by care givers, or analyzed by an insurance company. It has been said that health information, by its very nature, is particularly sensitive. The authors propose that ensuring its confidentiality is key because of the power a person or organization can wield over individuals by collecting, using, or disclosing this kind of information. Personal health

information may affect individuals' employment opportunities, their relationships, their entitlement to government and private services, pensions, and their very sense of well-being. Privacy advocates argue that feelings about health information can be very strongly held, because health information can contain very intimate details of an individual's life.

The fact that the way in which health information is treated can have such a profound impact on the life of an individual attests to the need for this report. The report examines the continuing debate on what right individuals have to control what happens to information about them. It looks at the views of key stakeholder groups in the debate, and some recent legislative responses. Those most affected by the outcome of the debate, the individuals whose health the information is about, are asked what they find to be the most important aspects of health privacy. Then these three perspectives are compared to discover what strengths and gaps there are in the present approaches.

Figure 1.3.1



From preliminary research in the literature and talking to experts, the researchers found that health information privacy raises fundamental questions about the circumstances in which it might be appropriate for health information to be shared: in order to receive direct care, for research, or to pay for care. It is evident that sharing information for the purposes of the provision of health care could be beneficial, with consent from the individual. Not sharing information can cause harm, for example when an individual's health care provider is unaware that another provider has prescribed some medication that is counterindicated in the current proposed treatment. There are yet other advantages that may be available through sharing information that don't involve such potentially catastrophic gaps in communication. Perhaps

sharing information might make it easier to get an expert opinion, either without having to resubmit to examinations, for example, or, by taking advantage of technology, getting that opinion from someone far away. Some amount of sharing is necessary in order for care-givers to be paid by public or private insurers. Research is another reason that information is shared (whether it attempts to track the instances of a particular disease, the efficacy of a particular therapy or review of prescription patterns). In each of these cases of health information sharing, the individuals to whom the information refers may or may not be asked about what they prefer, about how they wish information about themselves to be controlled.

The consultation about control of health information is central to privacy and is referred to in this report as the issue of consent. The majority of the discussion in the report consists of when consent can be implied, when it must be explicit[1] and when, if ever, it might be appropriate to allow the collection, use and disclosure of personal health information without consent. The report will also touch on other areas of health information privacy, such as the provisions and practices allowing individuals to access information about themselves. Also, it briefly discusses the systems established to provide redress if individuals believe their heath information privacy has been compromised.

1.4 Information flows

In order to come to grips with the issues for consumers regarding health information privacy, it may be helpful to look at the kind of challenges facing the health care industry with regard to information management. Central to the debate about health privacy is the flow of personal health information among health care system participants. These participants include, but are not limited to: health service consumers or patients, health care practitioners, facilities (such as hospitals and nursing homes), public insurance administrators, private insurers, researchers, private statistical data clearinghouses, and government agencies. Figure 1.3.1 illustrates the three key terms used to describe information flows among health care system participants. For example, a health care provider may collect personal health information from a patient and disclose such information to a third party (such as a researcher).

There is considerable discussion among health care system participants about which information flows should be allowed to occur among the participants, with or without patients' explicit consent, and what conditions should be placed on the related data transfers. In fact, there is little understanding of what exactly is "common practice" in part because the health care industry contains so many disparate players. Louise Sanchez-Sweatman offers five reasons why such an understanding is important.

First, transparency and openness are critical; "if the Canadian public is to know where their health information flows, then they need to be informed at the point of collection about what

[1] Implied and explicit consent are also referred to in some contexts as implicit and express consent. Although every effort has been made to use the former terms consistently in this report, in some cases (quotes, references) the latter may appear. They are to be understood to refer to the same concepts.

happens to their information."[2] Secondly, Sanchez-Sweatman suggests that "the right to privacy and individual dignity, autonomy, and freedom can only be ensured if individuals can control the flow of data. If there is a lack of clarity on where health information is traveling, then it is difficult to ensure that these principles are being respected."[3] Accountability, standards development, and policy development are three other reasons for having an increased understanding of health information flows.[4]

After conducting an extensive literature review on the topic, Sanchez-Sweatman developed a flowchart that maps health information flows within Canada. The flowchart is broken down into four levels. Level 1 involves an exchange of information during an encounter between a Canadian citizen and a provider, clinic, independent health facility, or a private commercial body. Level 2 includes information exchanged for health care service and follow-up. Level 3 information exchanges are for health care service payment purposes and level 4 exchanges are for non-clinical uses of health information.[5] Under this model, the information flows are categorized first by purpose, then by user.

Upon reviewing the types of information flows included in Sanchez-Sweatman's model, it becomes obvious why the debate among the health community on the subject of health privacy is yet unresolved. The reasons for which health information is needed are many and varied. The number of individuals and organizations potentially involved with the collection, use, access, disclosure, or retention of health information is considerable. Moreover, the ability to monitor authorized flows and uses of specific information among various parties becomes increasingly difficult and complicated as the amount of data exchanged or used and number of parties involved, or potentially involved, at any of the four levels increases. Furthermore, the authorization process itself, which involves demonstrating explicit or implied consent, is integral to the process yet has the potential to be an administrative nightmare if inappropriately administered.

1.5 Health privacy law in Canada

While both the federal and provincial levels of government in Canada have powers to regulate in the area of health, the delivery of health care in Canada is largely considered to be a provincial area of responsibility. The Canadian constitution gives provincial governments exclusive jurisdiction over hospitals, as well as "property and civil rights in the province" (including regulation of the medical profession), and "generally all matters of a merely local or private nature in the province". For this reason, most legislative activity in the area of health privacy has occurred at the provincial level.

[2] Louise Sanchez-Sweatman "Canadian Health Information: Where Does It Flow?"(1999) HC IM&C, 4th Quarter, , pp. 48-54.
[3] Ibid.
[4] Ibid.
[5] Ibid.

Three provinces - Manitoba, Saskatchewan, and Alberta - now have legislation governing the treatment of health records.[6] Ontario issued a consultation draft of such legislation in early 2002, after withdrawing a previous bill due to public outcry (including strong comments from the province's own Privacy Commissioner) over its privacy-invasive nature.[7] The Alberta law was also subject to a storm of opposition from the medical community as well as consumer groups. Criticism focused on (a) exempting private health care facilities from the scope of the Act unless they are providing an insured medical service paid for by Alberta Health; (b) the failure to meet the standard set by the Canadian Medical Association (CMA) Code; and (c) the absence of any public hearings. Despite strong and growing opposition, the Alberta government invoked closure to cut off debate and pass the bill only three weeks after it was introduced. To varying degrees, all of these statutes permit the sharing of personal health-related information amongst various types of health care providers. They are discussed in detail in section 5 of this report.

The Quebec *Act Respecting The Protection Of Personal Information In The Private Sector* was passed in 1994. It applies to all enterprises in Quebec, including private sector organizations which deliver health services, as well as any professional who operates a practice. While disclosure and secondary uses of personal information are subject to the requirement of informed consent under this statute, collection is governed by a different, less onerous set of rules.

At the federal level, legislation governing general data protection in the private sector came into force January 1, 2001. Part I of *The Protection of Personal Information and Electronic Documents Act* (*PIPEDA*) provides Canadian citizens with rights to control the collection, use and disclosure of their personal information in the context of commercial transactions. Specifically, it requires that any collection, use, or disclosure of personal information in the context of commercial activities be done only with the individual's knowledge and consent, subject to specific listed exceptions. The *PIPEDA* is cross-sectoral legislation and therefore does not deal specifically with health records. Rather, it establishes broad principles that can be applied in all sectors. Moreover, the *PIPEDA*'s application to commercial activities renders it only partially applicable to the health sector, which spans both commercial and non-commercial activities. In any case, even those who support the *PIPEDA*'s application to personal health information (privacy advocates and many health care stakeholder groups) recognize that, while the broad principles established by the

[6] Manitoba passed the *Personal Health Information Act* in late 1997; Saskatchewan passed the *Health Information Protection Act* in early 1999 though it is not yet in force
and Alberta passed Bill 40, the *Health Information Act* in late 1999 see also discussion in s.4.1 of this report.

[7] See http://www.cbs.gov.on.ca/mcbs/english/56HK6V.htm.

PIPEDA can be applied to the health sector, they are insufficient to deal with the unique challenges arising in that context.[8]

In addition to statutory law, the Canadian *Charter of Rights and Freedoms* offers some protection for personal health information. While the *Canadian Charter of Rights and Freedoms* does not contain an explicit right to privacy, the Supreme Court of Canada has confirmed in a number of cases that privacy rights are guaranteed by sections 7 and 8 of the *Charter*. It has recognized the highly private and personal nature of individual health records, noting that such information "goes to the personal integrity and autonomy of the patient" and is, regardless of where it is recorded or stored, in a fundamental sense, one's own.[9] In other cases involving the privacy of accused persons and witnesses, the Supreme Court has emphasized that privacy is at the heart of liberty in a free and democratic state.[10] In a recent judgement, the Court linked privacy with "security of the person" in section 7 of the Charter, ruling that the confidentiality of complainant medical records is essential to the therapeutic relationship, and that without a guarantee of such privacy, the individual's trust may be damaged and her security of the person undermined.[11]

As well as the statutes mentioned, and the common law, it must be noted that personal health information protection is affected by numerous other rules. There are codes of practice, professional ethics, rules and laws that apply to the health care sector, insurers and government, all of which influence how these players deal with personal health information.

1.6 Definitions

Much discussion on the issue of health information privacy might be unnecessary if there were a common understanding of the terms used to describe the issue.

We need better definitions of privacy, consent, personal health information, identifiable and de-identified health information, disclosure, access, and societal good. It is clearly important to come to a consensus on the meaning of these important terms since the consistent interpretation of voluntary codes, legislation, and regulations relies on such a common understanding.

For the purpose of this report, the following definitions will apply to the interpretation of these important terms.

Personal health information: This report uses a working definition that combines two statutory sources. The following definition is from the *PIPEDA*:

[8] See the Public Interest Advocacy Centre's paper: "Health Information Privacy Protection: Finding the Right Balance"(2002) the Public Interest Advocacy Centre
[9] *McInerney v. MacDonald*, [1992] 2 S.C.R. 138 at 148.
[10] *R. v. Dyment* (1989), 55 D.L.R.(4th) 503; *R. v. O'Connor* (1995), 130 D.L.R.(4th) 235.
[11] *R. v. Mills*, [1999] S.C.J. No.68, (QL).

> **"personal health information",** with respect to an individual, whether living or deceased, means information concerning the physical or mental health of the individual; information concerning any health service provided to the individual; information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual; information that is collected in the course of providing health services to the individual; or information that is collected incidentally to the provision of health services to the individual."[12]

The above definition taken out of context does not limit itself to personally identifiable information. In order for this report's working definition to do so, it also adopts the definition of personal health information from the draft Ontario Act, which elaborates on the concept of personally identifiable information:

> "… whether or not the information is recorded, …is information that, identifies the individual, can be manipulated by a reasonably foreseeable method to identify the individual, or can be linked or matched by a reasonably foreseeable method to other information that identifies the individual or that can be manipulated by a reasonably foreseeable method to identify the individual…"[13]

Therefore, for the purposes of this report, personal health information is defined by the combination of these excerpted definitions. For a full discussion of how personal health information is defined in the Acts, see section 5.3.

Privacy is notoriously hard to define, but this report focuses primarily on the control aspects of privacy, the working definition for the purposes of this report is therefore:

Health Privacy: Health privacy affords an individual control over who can collect, use and disclose information about his or her personal health information. It also provides the right for the individual to access and correct personal health information pertaining to him or herself, which is retained by organizations or persons.

Access to health information: means the ability to review, acquire, or possess health information in any information format.[14]

[12] PIPEDA definitions, s.2(1)

[13] ON s.2

[14] Adapted from CMA, Section B, definitions. This report refers to access in two circumstances: as the obverse of disclosure, for third parties; and individuals' access to information about themselves. When the report uses access in the second sense, access will always be modified to indicate that it is not referring to access by anyone other than the individual whose information is in question.

Collection of personal health information: Collection is the act of obtaining personal health information from any source, including the individual it pertains to or a third party, by any means.

Consent: Again, this report uses the Canadian Medical Association's Health Information Privacy Code definition: **""Consent"** means a patient's informed and voluntary agreement to confide or permit access to the collection use or disclosure of his or her health information for specific purposes"[15]. Consent is discussed at length in section 5.2..

Consent can be explicit (express) or implied (implicit). "**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**. "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 if it were sought."[16]

It is sometimes necessary to separate the purposes of the collection, use and disclosure of personal health information for clarity. In order to do so in this report, the Canadian Medical Association Health Information Privacy Code definitions were adapted.

Primary purposes: are directly related to the therapeutic treatment of a particular patient, and paying for that treatment.

Secondary purposes are those which do not fall under primary purposes.

Consumer / Individual / Patient: These terms are (usually) used to mean the person about whom personal health information is collected, used or disclosed. However, for the purposes of this report, the definition also includes a person acting on behalf of the subject individual, for example, a parent or caregiver of a child. Individual consumers hold perhaps the greatest stake in deliberations and policy about health information practices, and are therefore defined and treated separately in this report from other individual stakeholders.

Disclosure: "means the provision of health information to a third party for any reason, or making health information available for a third party to collect. It includes any transfer or migration from one provider or user to another."[17]

Health care provider: "A health professional or institution that delivers health care services."[18] The definition used in this report is meant to be inclusive, covering providers of alternative health care, such as acupuncturists and homeopaths, as well as the traditional western medicine practitioners.

[15] CMA Section B, definitions
[16] CMA, Section B, definitions.
[17] CMA, Section B, definitions
[18] CMA Health Information Privacy Code

Stakeholder groups: This term refers to the *groups* that: represent consumers or health care employers, providers, or workers; provide health care; conduct research with health information; pay for or insure health care; administer health care information; and government departments that deal with healthcare or health information privacy. It also refers to *individuals* represented by the above groups. This list of groups and individuals is intended to be illustrative, rather than comprehensive.

Use of health information: "means any processing of health information, including storage, retention, retrieval, manipulation, connection or linkage to other sources of information in any format."[19]

1.7 Key players in the health privacy debate

There are many agencies, organizations, committees, and individuals who, together, have shaped the health privacy debate to date. Presented below in alphabetical order is an overview of the mandates of a selection of stakeholder agencies, organizations, and committees that have played pivotal roles in the debate.

British Columbia Freedom of Information and Privacy Association (BCFIPA)

BCFIPA provides information and education on Freedom of Information (FOI) and privacy issues; acts as a legal research and policy resource on freedom of information, privacy and other information issues. It is British Columbia's major public watchdog for FOI and privacy issues, and the only advocacy group in Canada devoted solely to these issues. It also intervenes in key cases that come before B.C.'s Information and Privacy Commissioner.[20]

Canadian Institute of Health Information (CIHI)

CIHI is an independent, not-for-profit organization that plays a central role in the development of Canada's health information system. It's mandate is to coordinate the development and maintenance of a comprehensive and integrated approach to health information for Canada; and to provide and coordinate the provision of accurate and timely data and information required for: establishing sound health policy; effectively managing the Canadian health system, and generating public awareness about factors affecting good health [21]

[19] CMA, Section B, definitions
[20] Summarized from the BCFIPA website: **http://fipa.bc.ca/about/** accessed February 2002
[21] Excerpted from the CIHI website: **http://www.cihi.ca/weare/weare.shtml** accessed February 2002

Canadian Institutes of Health Research (CIHR)

CIHR is a federal funding agency that supports research in Canada. It is mandated by Parliament to, among other things, promote, assist and undertake health research that meets the highest standards of ethics.[22]

Canadian Medical Association (CMA)

The CMA is a national voluntary organization, founded in 1876, of individual member physicians. The CMA represents physicians' concerns at the national level. 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.[23]

Consumers' Association of Canada (CAC)

Founded 55 years ago, CAC is an independent, non-profit organization whose mandate is "to inform and educate consumers on marketplace issues, to advocate for consumers with government and industry, and work with government and industry to solve marketplace problems." CAC focuses its work in the areas of food, health, trade, standards, financial services, communications industries and other marketplace issues as they emerge.[24]

Health Canada

Health Canada "is the federal department responsible for helping the people of Canada maintain and improve their health. … In partnership with provincial and territorial governments, Health Canada provides national leadership to develop health policy, enforce health regulations, promote disease prevention and enhance healthy living for all Canadians."[25] The department administers the *Canada Health Act*.

Industry Canada

Industry Canada's mandate "is to help make Canadians more productive and competitive in the knowledge-based economy, thus improving the standard of living and quality of life in

[22] CIHR (2001). Ethics. **http://www.cihr.ca/about_cihr/ethics/ethics_menu_e.shtml** Accessed February 12, 2002.
[23] CMA (2002) who we are. **http://www.cma.ca/cma/menu/displayMenu.do?pageId=/staticContent/HTML/N0/l2/General/AboutCMA.htm** Accessed February 2002
[24] **http://www.consumer.ca/**
[25] Health Canada (2002). About Health Canada. from http://www.hc-sc.gc.ca/english/about/about.html Accessed February 26, 2002

Canada."[26] The department administers *the Personal Information Protection and Electronic Documents Act (PIPEDA).*

Privacy Commissioner of Canada

The Privacy Commissioner of Canada's role and mandate is best described by the following excerpts from the Commissioner's web site:

> "The Privacy Commissioner of Canada is an Officer of Parliament who reports directly to the House of Commons and the Senate. The Commissioner is an advocate for the privacy rights of Canadians with the power to: investigate complaints and conduct audits under two federal laws; publish information about personal information-handling practices in the public and private sector; take matters to the Federal Court of Canada; conduct research into privacy issues; and promote awareness and understanding of privacy issues by the Canadian public."

The Commissioner hears and investigates complaints filed by Canadians with regards to Section 29 of the *Privacy Act* and Section 11 of *the Personal Information Protection and Electronic Documents Act*. George Radwanski was appointed Privacy Commissioner of Canada on October 19, 2001and is serving a seven-year term.[27]

Privacy Working Group

The Privacy Working Group (PWG) was comprised of representatives from the following six national associations: Canadian Dental Association, Canadian Healthcare Association (which represents healthcare facilities and agencies), Canadian Medical Association, Canadian Nurses Association, Canadian Pharmacists Association, and Consumers' Association of Canada. The Group's activities were funded by a small grant from Health Canada, which expired in March 2001.

Public Interest Advocacy Centre (PIAC)

PIAC seeks to advance the interests of individuals and groups who are generally un-represented or underrepresented in issues of major public concern. Founded in 1976, PIAC champions those issues that involve the delivery of important public and utility services. The Centre undertakes legal and research services on behalf of consumers. The Centre focuses primarily on consumer issues concerning telecommunications, energy, privacy, the information highway, electronic commerce, financial services, broadcasting, and competition law.[28]

[26] Industry Canada (2001). Mandate. Updated August 3, 2001. from http://www.ic.gc.ca/cmb/Welcomeic.nsf/ICPages/Mandate Accessed on February 26, 2002
[27] Privacy Commissioner of Canada. Updated February 26, 2002. About Us. from http://www.privcom.gc.ca/au_e.asp Accessed on February 26, 2002
[28] exerpted from the PIAC website: www.piac.ca

Standing Senate Committee on Social Affairs, Science and Technology

The mandate of the Committee is to examine legislation and matters relating to social affairs, science and technology generally. Included among the eleven areas are health and welfare matters[29]. Several witnesses, including a number of representatives of the health community, appeared before the Committee in he matter of Bill C-6 (later amended and passed as *the Personal Information Protection and Electronic Documents Act*). The Chairman of the Committee is Senator Michael Kirby.

1.8 Research themes

While there are many issues that are worthy of research in the health privacy arena, it was not practical to examine every issue for the purposes of this study. Instead a limited number of issues were carefully selected for in-depth exploration. An introduction to each of these issues follows.

1.8.1 Consent

Three research themes related to consent are explored in this study: the impact of non-harmonized health privacy protection on consumers; the appropriateness of requiring explicit consent or assuming implied consent for a variety of secondary purposes; and, consumers' understanding and perceptions of the risks and potential consequences of withholding or granting consent.

The review of legislation undertaken for this report attempts to identify the inconsistencies, particularly in the rules relating to consent, which may greatly impact consumers. There is a need to develop procedures and standards that outline the mechanisms for requiring consent. The research in this study attempted to answer the following questions relating to the issue of consent:

- When is explicit consent practical and value-added?
- When is it appropriate to imply consent?
- For how long does consent last?
- Is consent for primary use different from consent for secondary use? Do patients have to give consent separately for both cases?
- Does blanket consent constitute informed consent?

For consent to be truly informed, care recipients need to understand the risks and consequences of withholding or providing consent. This includes knowing and understanding

[29] Parliament of Canada (2002). Mandate. Accessed February 26, 2002 from http://www.parl.gc.ca/common/Committee_SenHome.asp?Language=E&Parl=37&Ses=1&comm_id=47

the conditions of collection, access, disclosure, and use to which they are consenting. The research in this study attempted to determine whether or not consumers understand the potential implications of providing or withholding consent. It also attempted to ascertain how consumers feel their personal health care and societal welfare might be affected by providing or withholding consent to collect, use, access, or disclose their personal health information for primary or secondary purposes.

1.8.2 Health system knowledge dissemination

It was suggested in the above discussion about information flows (section 1.4) that there is a lack of awareness among regulators, providers, and the public about current practice and daily intersects among multiple payers, suppliers, and consumers. Fear of the unknown breeds uncertainty, skepticism, and worry that abuses of the system occur and will continue to occur when properly administered controls are not in place. Moreover, there are concerns that abuses will go undetected until serious and irreparable damage has been done to an individual's privacy.

The lack of a common basis of understanding and knowledge regarding how the system works impedes the development of solutions for health privacy concerns. The first step to address this challenge is to determine the current level of understanding in the community regarding how information flows through the health system. The consumer research conducted as part of this study attempts to bring to light consumers' beliefs, experiences, and fears, probing for both awareness of and experience with personal health information flows.

As an adjunct to the above research, consumers were also asked to whom they are currently giving implicit or explicit consent for the use of their personal health information. It was recognized, however, that given the time and resource limits imposed on this study this research theme could only be explored cursorily. In addition to researching consumers' awareness of information flows, consumers' perceptions of how their personal information is currently being used was also explored.

1.8.3 Redress

As will be noted later in the study report, the Standing Senate Committee on Social Affairs, Science and Technology has accepted the Minister of Health's and the Privacy Commissioner of Canada's argument that the privacy of consumers' personal health information is adequately addressed. The Committee argues that consumers have appropriate recourse through the Privacy Commissioner's complaints handling system should a health privacy breach occur. Consumer representatives argue that this is not the case; the redress mechanism available through the Privacy Commissioner is a reactive rather than proactive approach.

Part of this study involved conducting primary research to test the consumer advocates' argument. The purpose was to ask consumers what recourse they feel they currently have,

whether consumers feel the current redress mechanisms are appropriate, and what procedures and policies should be in place that would prevent any privacy breaches from occurring in the first place. The research also sought to determine whether stakeholders believed reasonable penalties should be imposed for privacy violations and, if so, what penalties would be appropriate.

2 Methodology

2.1 Methodological framework

The primary aim of this report is to advance a well-researched consumer position on the current debate regarding the privacy of personal health information (PHI). To provide a framework within which to better understand the implications of consumer views, research was undertaken to set out as clearly as possible the current legislative environment surrounding personal health information, detailed in section 2.3.4, and to clarify and synthesize the positions held by stakeholder groups on the issues, detailed in section 2.3.2 below. Issues identified in these two contexts were highlighted and formed the basis for eliciting consumer views through qualitative focus groups and a quantitative survey described in section 2.3.3. Consumers were also encouraged to bring to the table additional issues not identified in the background research if they considered them to be relevant. Results from the three perspectives, set out in sections three through five, are compared in section 6 and divergences of views and perceived gaps in the protection of personal health information are identified. Recommendations are provided to address those gaps.

2.2 Research of positions held by stakeholder groups

2.2.1 Rationale

Consumers, as clients of the health system, clearly have the most at stake in the application of legislation and regulations concerning health privacy. However, healthcare practitioners, facilities, researchers and administrators also have much at stake; they provide important inputs to the health care system that allow consumers to benefit from health services. Certainly, these other stakeholders are also directly affected by rules governing health privacy practices and policies.

As noted in the report introduction, national organizations and agencies, representing health system participants, have been actively voicing their concerns about the implications of requiring health privacy specific legislation to apply to their individual and organization members. As they are responsible for complying with health privacy legislation, it is important to understand and properly consider their concerns, arguments, and recommendations.

A well-informed consumer position cannot be formulated without considering and understanding the position of other stakeholders. Therefore, in lieu of researching and analyzing consumers' views in isolation, an initial review of other stakeholder positions was conducted to provide a benchmark against which consumer views could be compared and

contrasted. The terms "stakeholder groups" "stakeholder organizations" are used interchangeably through the report.

2.2.2 Selection of stakeholder groups

The following organizations and agencies were selected as they represented the key stakeholder groups. Their selection was intended to try to represent the most divergent views and include a wide range of opinions. The groups represent consumers or citizens, healthcare practitioners, and researchers: There may be other groups involved in the privacy of health information debate, however, these groups were ones which actively participated in the senate hearings in 2000 and had published position papers available to the researchers for this report. The groups that were chosen are: BC Freedom of Information and Privacy Association (BCFIPA), Canadian Institutes of Health Research (CIHR), Canadian Medical Association (CMA), Consumers' Association of Canada (CAC), Privacy Working Group (PWG), and Public Interest Advocacy Centre (PIAC).

2.2.3 Literature review and personal communications

In considering the positions of the stakeholder groups selected for this study, a number of resources were consulted. These documents included: policy statements issued by the organizations; letters sent by and among the stakeholder organizations; materials prepared for or as a product of workshops and presentations; submissions to senate committees; senate committee reports; and other relevant background documents published in newspapers, magazines, and academic journals or as printed or electronic stand-alone works. These resources are referenced in the report bibliography.

Where there was a need to clarify a stakeholder organization's position, representatives of the organization were contacted personally. Information gathered at privacy-related conferences and during informal personal communications was also used to enrich the researchers' understanding of the health privacy debate.

2.2.4 Issues review for stakeholder group positions

The issues reviewed for the stakeholder group positions are essentially the same ones used to review the statutes. The issues are discussed at length in section 1.8. They can be grouped into three general areas of review: consent, health system knowledge dissemination and redress.

2.3 Research on Consumer Views

2.3.1 Rationale

As set out in section one, the issue of the privacy of personal health information is a complex one comprising several related and subsidiary issues that make a simple poll of Canadian views on these questions inappropriate and likely uninformative. Instead CAC and PIAC chose to survey a small sample of Canadian consumers from coast to coast using a more detailed questionnaire. This was complemented by several regional focus groups in which key information required to participate in this debate was provided to those attending the sessions. As mentioned above (in section 1.2), since CAC and PIAC have also been active stakeholders in this debate an impartial consulting firm, The Action Group (TAG) was sub-contracted to collect and analyze consumer data to ensure impartiality and a balanced perspective. In the context of an open, neutral stance with regard to the issues at hand, TAG elicited a range of views from Canadian consumers that inform this ongoing debate along the following lines.

- Awareness of the issue

Although every Canadian has personal health information and is thus implicated in this debate, it is far from clear to what extent this issue is salient to most consumers. Do Canadians ever think about the protection of their personal health information? Are they aware of what safeguards are in place? Do they understand what the current practices are with regard to consent, disclosure and flow of personal health information?

- Importance of the issues surrounding the privacy of personal health information

If aware of some or all of the issues in this debate, what importance do Canadians place on the issues and on the privacy of their personal health information? Do they feel these are central policy issues that require more attention from government and regulatory bodies, or are they peripheral to other more salient issues in health or consumer protection? Within the scope of privacy and personal health information, which of the many subsidiary issues are of greatest concern to the Canadian consumer? For instance, is there greater concern over the use of personal health information in research or over the issue of consumers' ability to access their own personal health information?

- Scope of the debate

As noted in section 1.6, the Privacy Work Group, in its year-long debate set out the parameters of the discussion and highlighted several core and ancillary issues relating to the privacy of personal health information. Do Canadian consumers concur with the scope of this framework or are there issues of central importance to Canadians that have not been raised? If so, what are these issues and why are they so important to the consumer?

- Proposed adjustments to the current levels of protection of personal health information

What measures do Canadian consumers believe should be in place to ensure the protection of their personal health information? How stringent should consent requirements be? How should they differ to reflect the proposed use of their personal health information? Are there any innovative perspectives among consumers that might open new approaches to managing personal health information?

2.3.2 Data collection

A combined qualitative/quantitative approach was adopted to address the above questions based on the view that qualitative data is best suited to eliciting details on the *nature* of consumers' concerns, that is, to allow a sufficiently open-ended format to permit issues not necessarily previously addressed to surface and then to explore these and previously identified issues in some depth. Quantitative data, on the other hand, provides some indication of the *relative importance* of the issues to Canadian consumers as a whole, and whether regional or other demographic differences should be considered.

2.3.2.1 Qualitative Data: Focus Groups

During February, 2002, focus groups were conducted across Canada with residents of four provinces, Alberta, Manitoba, Ontario and Quebec, three in English and one in French. The groups comprising residents of Ontario and Quebec were divided along linguistic lines rather than by place of residence, so there was one English-speaking resident of Quebec in the Ontario group and two French-speaking residents of Ontario in the French group. For ease of reference, these two groups are referred to as the Ontario group (= Anglophone) and Quebec group (= Francophone), but the reader should be aware of the small demographic overlap.

A fifth focus group was conducted earlier in Ottawa as a preliminary test of the focus group methodology. Since that group responded well to the prompts, handouts and the subject in general (see Appendix C1), no substantive changes to the methodology were introduced. Given the timeline for this study, which restricted the overall number of focus groups to be held and the fact that subsequent focus groups were conducted in the same way, it was decided *post hoc* to include the results from this preliminary group discussion in the results section[30].

Forty-nine participants were recruited by word of mouth from networks of previous survey participants, research contacts, second-hand referrals and a newspaper advertisement in the local French daily newspaper, *Le Droit*. Since individuals for these groups were to be representatively and not randomly sampled[31], participants were selected to correspond to

[30] Results from this session are identified as being from the "preliminary focus group". The subsequent inclusion of pilot data in final results when no methodological changes are introduced as a result of the pilot study is not uncommon in social sciences research.

[31] Focus groups cannot serve as randomized samples for inferential statistics since no extrapolation to the wider population would be warranted based on such a small sample (often only a single

three principal demographic variables: gender, age and education. Attempts were also made to include rural participants, although weather and budgetary constraints precluded their participation, making this an urban and sub-urban sample. Participant demographics are summarized in Table 2.3.2.1.

Across all five groups, the occupations of the participants varied widely, including, among others, a librarian, teacher, businessman, representative of the armed forces, manager, receptionist, public servant, artist, homemaker, student and three retired individuals. Eleven individuals were caring for children, only one for an elderly relative.

Data from the focus groups were analyzed qualitatively, with an emphasis on themes and disparate views regarding key issues among participants. Regional differences are noted, but should be interpreted with caution given the small number of participants in each group. Results are set out in section five.

Table 2.3.2.1
Focus Group Participants

	Prep	**AB**	**MB**	**ON**	**PQ**	**Total**
Total by Group	10	9	10	11	9	49
Gender						
male	6	3	5	4	3	21
female	4	5	3	7	6	25
unspecified[32]	0	1	2	0	0	3
Age						
under 20	0	0	2	0	0	2
20-39	8	3	0	6	3	20
40-59	2	3	3	3	6	17
over 60	0	2	3	2	0	7
unspecified	0	1	2	0	0	3
Education[a]						
high school	0	2	4	2	2	10
college/vocational	2	2	0	3	3	10
undergraduate univ.	7	2	3	3	2	17
graduate university	1	1	1	3	2	8
unspecified	0	2	2	0	0	4

a. respondents were asked to specify the highest level of education completed. None chose the option 'grade school'.

representative for any given demographic). Therefore participants are chosen to *represent* their demographic in an attempt to widen the discussion and promote the inclusion of issues of relevance to sub-groups in the population.

[32] Demographics were collected as part of the summary questionnaire at the end of the sessions. Individuals who chose not to complete this portion were deemed unwilling to share their demographic information and thus it has not been included even where known (e.g., gender).

2.3.2.2 Quantitative Data: Written Survey[33]

To encourage cross-Canada participation in such a short time frame, quantitative data collection focused on email solicitation of consumer views. Messages were posted to a wide variety of newsgroups and listserves asking individuals interested in the topic to request a copy of the survey by email. This was supplemented by advertisements in several rural West Coast newspapers (since no focus groups were held in British Columbia) and to ensure some rural participation in the debate. Participants contacted for another cross-Canada survey being conducted by TAG for CAC (on laser eye surgery) were also asked if they were interested in participating in this survey. Participants were given a choice to complete the survey electronically or to print it out, complete it, and return it via standard mail. Finally all focus group participants were also asked to fill out the survey at the end of their focus group sessions.

What was evident from the survey data received was that while only a limited number of consumers participated, those that did, did so thoughtfully. Despite the complex nature of the survey almost all of the responses received via mail (or email) were complete and reflected a care in responding that is not always evident in such surveys. This was indicated by the fact that although different responses were required for different questions (scaled responses: 0 - 5 vs. checkmarks vs. alphabetic responses: A, N, R) virtually all mail-in respondents used the correct type of response in the appropriate question. Ironically it was some of the focus group participants, particularly those over 60, who had greater difficulty, perhaps finding the cognitive load somewhat too great after a two-hour discussion or because of literacy issues. For that reason, sample size varies slightly in section 5, as not all responses were available for all participants.

Since the focus group participants did complete the questionnaire after two hours of discussion on the subject, they were considered 'informed' respondents and all quantitative responses were compared statistically with those of less informed respondents from other sources. Where there were no statistically significant differences, the sample was analyzed as a whole. Where differences were evident, these are noted and the two samples were not collapsed. The deadline for a response to the survey was March 8, 2002. All respondents who completed the survey by this date were entered into a $250.00 draw, which resulted in a winner from Ontario.

Data from the survey were analyzed quantitatively and conclusions drawn were used to elaborate or attenuate findings from the focus group qualitative data. Narrative segments in the email survey were reviewed for themes and for any new, previously unidentified concerns. These were linked to the qualitative data in the focus group sessions. Results are set out in section five.

[33] A copy of the written survey is provided in Appendix B.2. Some variations in survey format were necessitated for email transmission. The version supplied here is that completed by focus group participants.

In all 42 surveys were received from across Canada, which, combined with input from focus group participants, provided a total sample of 91[34]. This is clearly not a large sample and was well under the number expected, despite the short time frame (5 weeks) for data collection. Given other similar surveys conducted in the past and one on a different issue being conducted concurrently, all of which resulted in significantly higher interest levels, we might conclude that privacy and personal health information is not an issue that is foremost in the minds of Canadians[35]. This was supported by the many comments at the end of the survey and among focus group participants that this was the first time they had thought about the question. Equally frequent were comments to the effect that it is an important issue and that people need to be more aware of the implications of more or less privacy for their personal health information, further suggesting that one of the main challenges in this debate will be to better educate the public.

Despite relatively small numbers, the responses received were from a variety of regions, covering several age groups and careers and thus may be viewed as a diverse sample that provides a valuable consumer perspective on the issue (see table 2.3.2.2.). Extrapolation to the wider Canadian consumer population is not warranted, however, although consistencies in responses from different regions and different demographic characteristics may be taken to suggest the likelihood of widespread agreement pending further research. See Figures 2.3.2.1 and 2.3.2.2 for an overview of the sample as a whole.

[34] This number includes the 8 Francophone focus group participants who did not complete a full survey, but did contribute to the discussion of the issues. There were insufficient funds (and time) to allow for a reliable translation of the survey, so Francophone input was restricted to focus group participation and to the three individuals who were comfortable completing the survey in English In all, 83 surveys were available for analysis.

[35] It has been suggested that the term "privacy" may not truly reflect the extent of this issue, perhaps underplaying it in the minds of Canadians: the security and/or protection of information may be more central, or it may even need to be reconstrued as an issue of human rights: the right to have a say in what happens to one's personal information.

Table 2.3.2.2
Mail-in/Email Survey Respondent Characteristics

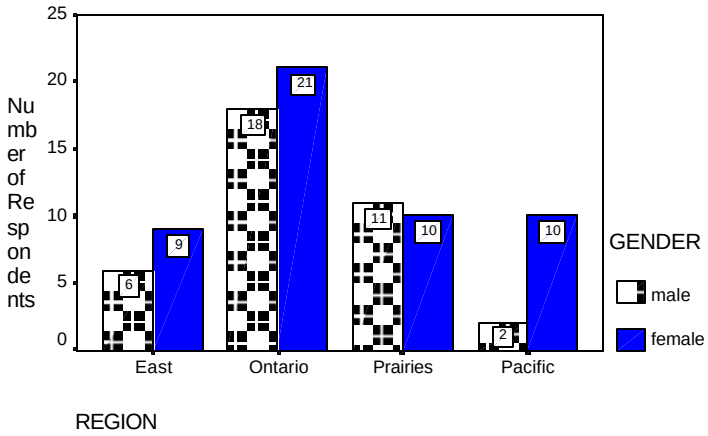
	East [a]	Ontario	Prairies	Pacific	Total
Total by Region	7	20	4	11	42
Gender					
male	3	8	2	1	14
female	4	11	2	10	27
Age					
under 20	1	0	0	0	1
20-39	3	16	0	5	24
40-59	3	4	4	6	17
over 60	0	0	0	0	0
Education					
high school	3	5	0	0	8
college/vocational	0	1	3	4	8
undergraduate univ.	0	6	1	5	12
graduate university	4	8	0	2	14

Quebec and the Atlantic provinces. Quebec was not distinguished as a separate region among the survey respondents, given that the survey was only available in English.

Figure 2.3.2.1

Overall Sample Characteristics: Region and Gender

(87 responses, 4 unspecified)

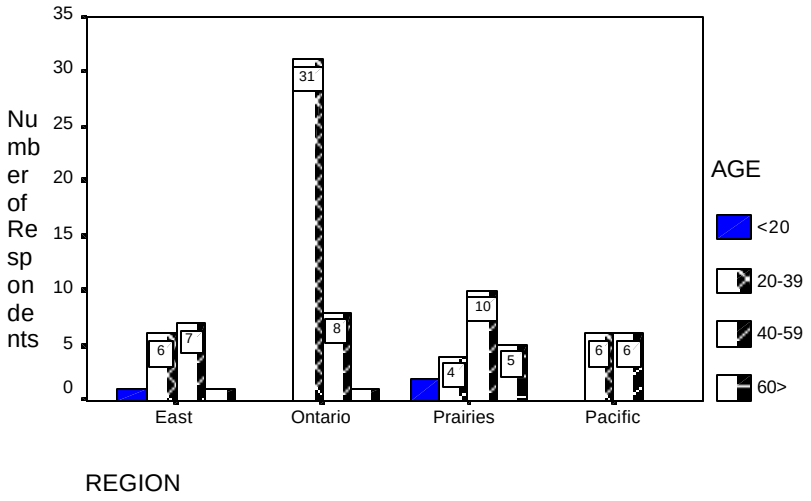


Occupations of participants ranged widely, including student, accountant, teacher, civil servants, clergy, retail, clerical workers, finance, engineering, lawyer, nursing and retired individuals. The higher number of more educated individuals is probably a function of the mode of data collection (internet, email). In Ontario respondents were much more likely to be in the 20-39 age bracket. Twenty per cent of the sample participants were caring for children and twenty per cent for elderly adults.

Figure 2.3.2.2

Overall Sample Characteristics: Region and Age

(87 responses, 4 unspecified)



2.4 Research of Canadian statutes

Section 5 of this report compares the Alberta, Manitoba, and Saskatchewan Acts concerning Health Information Privacy, as well as the draft Ontario privacy legislation and the *PIPEDA*. The Statutes are compared with regard to how they deal with a number of issues. Discussion about each issue for all of the Acts follows, in section 5.4.

Jurisdiction and Acts, with important dates		
Alberta	*Health Information Act*	Passed 1999
Manitoba	*Personal Health Information Act*	Passed 1997
Ontario	*Privacy of Personal Information Act*	**DRAFT** - 2002
Saskatchewan	*Health Information Protection Act*	Passed 1999 - **Not yet proclaimed**[36]
Canada	*The Protection of Personal Information and Electronic Documents Act*	In force (generally) January 1, 2001 January 1, 2002 for health information.

The statutes reviewed in this section were chosen for two main reasons. First, it was intended that the primary research results of this project would be compared to new provisions in health privacy statute law. The laws had most recently changed (or were about to change) in Alberta, Manitoba and Ontario. Accordingly, the relevant statutes of those provinces were reviewed, and the new draft Ontario privacy legislation, as well as a comparable statue in Saskatchewan.

Secondly, there is a wide range of statutory protections in Canada, but there is an emerging group of laws that are intended to be similar to each other. The review was intended to test how similar the protections they offered to consumers really were. Although the *PIPEDA* engendered so much concern when it became generally known that it would directly affect practices in the health care community, it is the model for the new legislation emerging. The provincial Acts reviewed were undertaken with an eye to being deemed substantially similar to the *PIPEDA*, so that the *PIPEDA* would not have jurisdiction in those provinces. If there is no substantially similar legislation in place in the provinces, in 2004 the *PIPEDA* will apply.

Another factor that influenced the choice of statutes reviewed are that although other provinces have some provisions in the area, their Acts were not specifically designed to cover target the entire medical community in the province. For instance, while the Quebec *Act Respecting the Protection of Personal Information in the Private Sector* applies to private sector health professionals, it does not have application to provincial hospitals. The British Columbia *Freedom of Information and Protection of Privacy Act* only covers access and privacy issues within the public bodies in the province, and not private health care professionals. The Acts chosen to be reviewed, on the other hand, are comprehensive in their coverage of personal health information in their jurisdictions.

[36] "Bill 29, *The Health Information Protection Act*, was tabled in the Saskatchewan Legislative Assembly on April 23, 1999. On May 6, 1999, the Lieutenant-Governor gave Royal Assent to *The Health Information Protection Act*. However, the Act does not come into force until proclamation, which has been delayed to allow time for trustees to prepare for compliance." – from the Saskatchewan government website: **http://www.health.gov.sk.ca/ph_br_health_leg_hipamain.html**

2.4.1 Issues reviewed in statutes

Issues reviewed in the statutes are the same ones which were reviewed for the analysis of stakeholder groups. They are discussed at length in section 1.8, Research themes.

2.5 Methodological Review

An expert in research methodology was retained by CAC to ensure the study's methodology was sound within the constraints imposed by the limited time frame and funds. The evaluator also ensured that interpretation of the results was warranted, based on the methodology chosen.

2.6 Methodological Limitations

It must be recognized that the issues surrounding the privacy of PHI are sufficiently complicated to preclude a comprehensive representative sampling of Canadian consumer opinion in a five-week data collection initiative. Rather than attempting data collection on a few issues that might permit representative sampling, the researchers chose to explore in greater detail core issues raised in the debate. Future quantitative research will be needed to clarify to what extent these views are truly representative of all Canadians.

Due primarily to time constraints that precluded translation, the email survey was only available in English. A Francophone perspective on this debate was elicited in a French-language focus group, although only participants comfortable in English completed the survey at the end of the session.

Perhaps the single greatest challenge in this research was to attempt to elicit clear and precise views on a subject that is neither clear nor precise. Since the research was to identify current consumer awareness of privacy protection, but also explore Canadians' perceptions of the issues raised in the debate and their vision of how they would like their personal health information protected, a careful balance was needed between surveying and informing. How consumers met this challenge is set out in section four.

3 Analysis of positions held by stakeholder groups

The following analysis addresses the substantial health privacy issues discussed above, in section 1.8, Research themes, in the position statements or similar documents from each stakeholder group reviewed. As mentioned in the Methodology, subsection 2.2.2, the stakeholders reviewed are listed. The stakeholder groups reviewed are: BC Freedom of Information and Privacy Association (BCFIPA), Canadian Institutes of Health Research (CIHR), Canadian Medical Association (CMA), Consumers' Association of Canada (CAC), Privacy Working Group (PWG), and Public Interest Advocacy Centre (PIAC).

The analysis is organized into several discussion themes: the meaning and expiry of consent, data retention and protection considerations, the need to demonstrate consent to collect, use, access or disclose personal health information, the use of personal health information for research purposes, patient access to data, and redress provisions. Each of these themes is discussed in turn.

3.1 Meaning of consent

In theory, the concept of consent should not be subject to much controversy. Consent may be deemed to exist when an individual voluntarily yields to what is proposed or desired by another[37]. Stakeholder groups, with the exception of researcher representatives, generally agree on the circumstances where consent is required before individuals' personal health information may be collected, used, accessed, or disclosed. However, stakeholder groups do not always agree whether such consent needs to be given explicitly or whether one could reasonably imply that consent exists, or when, if ever, consent is impracticable. This subject has been widely debated amongst the stakeholder groups, and, as will be demonstrated, they have not reached agreement on the topic.

Similarly, stakeholder groups agree that a patient's explicit consent should be informed but there is no agreement on what it means for a patient to be informed. Most of the stakeholder groups considered in this analysis have left the concept open to interpretation. The Privacy Working Group attempted to seek clarification on this point by asking other stakeholders to explain what it means to be informed. The group asked: whether informed consent requires direct verbal communication with an individual; whether written communication directed to an individual detailing procedures concerning consent was considered sufficient; or, whether written communication to groups of individuals, such as a bulletin board notice, was adequate. It is unclear whether any responses to this question were received.

By reviewing the positions of other stakeholder groups, some examples can be found as to what might be construed to be informed consent. For instance, the BC Freedom of

[37] Adapted from the *Funk & Wagnalls Canadian College Dictionary(1989)*

Information and Privacy Association notes that individuals have the right to "be told why specific information is requested and if it will be part of a physical record". Individuals also have the right to "know who will have access to any of [one's] health information and for what purpose"[38].

The Canadian Medical Association (CMA) offers a broader definition, as noted in clause 4.4 of CMA's Health Information Privacy Code:

> "Patients must either have, or by reasonable means be provided with, knowledge about what can or must happen with their health information. The degree of detail or specificity of this knowledge is what could be presumed germane to the decision of a reasonable person in the circumstances of the patient."[39]

Moreover, the Code further states:

> "to satisfy the requirement that consent be informed, the patient must have, or by reasonable means be provided with, knowledge about the potential for subsequent nonconsensual collection, use, disclosure or access before he or she confides any information.'[40]

This clause suggests that patients should be informed of any consequences of withholding consent and of any benefits of giving consent before explicit consent is sought. From the documents available, it appears that some of the groups representing health researchers also endorses this concept[41], as noted in Article 2.4 of the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans:

> "…researchers or their qualified designated representatives shall provide prospective subjects with the following: …
>
> (c) A comprehensible description of reasonably foreseeable harms and benefits that may arise from research participation, as well as the likely consequences of non-action, particularly in research related to treatment,

[38] BC Freedom of Information and Privacy Association. Declaration of Medical Privacy Rights. May 2001.

[39] Canadian Medical Association *CMA Policy Summary: Health Information Privacy Code*, CMAJ, October 20, 1998, at 997, 1003.

[40] *Id*. at 1003, principle 5: consent.

[41] The Medical Research Council of Canada, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada jointly prepared guidelines for health research. By making a linked reference to these guidelines on its web site, it appears that CIHR endorses these guidelines, collectively drafted as the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans.*

> or where invasive methodologies are involved, or where there is a potential for physical or psychological harm"[42].

While the above examples are not entirely contradictory, it is clear that there is no recognized standard for defining what it means for consent to be informed. As well, there is a lack of documented discussion about individuals' powers to limit the scope or duration of their consent. If individuals are asked to consent to the collection, use, disclosure, or access of personal information for secondary purposes, should they be allowed to place limits on the purposes for which the information will be used? Or similarly, should they be able to place access, use, or disclosure restrictions on the bodies that may have an interest in their personal information?

The BC Freedom of Information and Privacy Association believes that a number of "layers" of consent options should be presented to patients on a consent form. The form would be prescriptive, detailing the different types and depths of information sharing to which patients may choose to consent, or not. The patients would then designate a custodian, such as their physician, who would administer the patients' wishes[43].

Many of the stakeholder groups note that consent should be voluntary but, unlike the BC Freedom of Information and Privacy Association, they neglect to outline how individuals should give consent in practice. Moreover, further discussion is needed to resolve individuals' questions about how they can be assured that they will receive treatment while exercising their right to withhold consent to the collection, use, disclosure, or access of their personal health information for purposes unrelated to primary care.

3.2 Duration of consent

Clarity is thus clearly lacking about the meaning of informed consent, as well as the options that should be available to individuals to exercise their right to voluntarily provide or withhold consent. The authors of this report see these issues as important and requiring resolution. By comparison, however, the issue of duration of consent has stirred a more heated debate.

The position taken by the Canadian Institutes of Health Research (CIHR) stands in stark contrast to that of the other stakeholder groups. The assumption that can be inferred from the CIHR position is that research is a public good in itself, at least as valuable as privacy.

---

[42] Medical Research Council of Canada, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (August 1998), page 2.1. *available at* **http://www.nserc.ca/programs/ethics/english/policy.htm** Accessed February 5, 2002. It is notable that this policy statement is under revision.

[43] E-mail from Darrell Evans, Executive Director, BC Freedom of Information and Privacy Association, to Jennifer Shepherd, Research Analyst, Public Interest Advocacy Centre (31 January, 2002) (on file with the recipient).

According to CIHR, information made available to researchers for a given purpose may be used if required later for other purpose(s); it is not always possible to anticipate secondary uses of data that are of benefit to society. It is their position that where it may, at that later date, no longer be feasible to obtain consent to use the information, the benefit of proceeding with the secondary uses could outweigh the potential risks of infringing on individuals' privacy and acting against individuals' wishes.

A careful review of the positions held by stakeholder groups reveals, though, that the majority of the stakeholder groups believe there should be clear limits as to how long consent lasts to collect or access, use or disclose personal health information. The Consumers' Association of Canada's (CAC's) position on this issue is articulated in the association's Policy Statement on Protection of Personal Health Information: "Consent is continual and the consumer has a right to deny consent at any time."[44] However, as noted in another clause, it is clear that such continual consent only applies to circumstances that are consistent with the purposes to which individuals have already explicitly consented in writing:

> "… An organization or information custodian will collect only that information required for the purpose that was identified. If the information custodian wishes to use the information for purposes other than those originally identified the custodian must obtain the expressed written consent from the consumer prior to using the information."[45]

This position taken by CAC is reflective of the majority position taken by stakeholder groups: consent to collect, access, use, or disclose personal health information should expire at the time the authorized purposes have been concluded. There is, however, still a need to resolve the difference in opinion between this majority of stakeholder groups and the research community to reach consensus.

3.3 Data retention and protection

3.3.1 Data retention

A similar disagreement exists between CIHR and other members of the health community on the issue of data retention. The Institutes argue that it would be a waste of public funds to automatically destroy data and/or all possible identifiers after satisfying the original purpose(s) for which the data were collected or accessed. Moreover, "having to re-create new data archives for each new research project would be completely impossible and/or

[44] Consumers' Association of Canada,. Policy Statement on Protection of Personal Health Information, 3 (2001).
[45] *Id*

entirely cost-prohibitive."[46] This argument is contingent upon CIHR's other point that suggests data used for one purpose can be of social benefit when used for research purposes undetermined at the time of data collection or access. The contrary position is taken by the BC Freedom of Information and Privacy Association, the Consumers' Association of Canada, the Canadian Medical Association, and the Public Interest Advocacy Centre, who all agree that health information should only be retained for as long as it is necessary to fulfill authorized purposes.[47]

This debate highlights the discord in the community that pits advocates for individual privacy interests against advocates for accessible research data. To illustrate the debate, imagine a continuum with absolute individual privacy protection at one end and absolute access to personal information at the other. At one extreme, restricting access to personal health information can negatively affect the quality of the therapeutic relationship between a patient and his or her medical practitioners. It also means that society would not benefit from important research that may cure disease. At the other extreme, unquestioned access to personal health information has drawbacks, too. It compromises the confidentiality of the doctor-patient relationship and poses social risks and barriers to individuals when their personal information is used for inappropriate purposes. However, it allows responsible researchers to delve into data that can be used to identify trends and make important medical discoveries.

3.3.2 Data protection

While the debate continues among the health community as to how long data should be retained, there is no disagreement about how the data should be retained. All stakeholder groups agree that appropriate security safeguards need to be in place to protect the integrity of the data in the hands of information custodians, including medical practitioners, administrators, and researchers. The Canadian Medical Association's Health Information Privacy Code, for example, recognizes security as one of the ten overarching principles and provides specific and detailed requirements:

> "8.6 Security safeguards shall include both physical and human resource safeguards to prevent unauthorized health information collection, use, disclosure and access. Physical security measures include such safeguards as locked filing cabinets, restricted access to certain offices or areas, and the use of passwords, encryption and lock-boxes. Human resource

[46] Canadian Institutes of Health Research, Draft case studies involving secondary use of personal information in health research (December 2001) at 12.
[47] BC Freedom of Information and Privacy Association, *Supra*, note 38, h; Consumers' Association of Canada, *Supra* note 44, 5-6;
Canadian Medical Association, *Supra* note 39 clause 3.10

> security measures include security clearances, sanctions, training and contracts."[48]

The Consumers' Association of Canada further notes that effective security safeguards must address authentication, integrity, and non-repudiation concerns.[49] The range and complexity of available safeguards will continue to change with ever-increasing technological advances. The challenge is to ensure that the minimum standard for securing personal information is flexible but sufficiently rigorous to ensure meaningful protection.

3.4 Consent to collect, use, or access personal health information

The above analysis showed that stakeholder groups are divided on the controversial issue of where the balance between privacy and access needs to be struck regarding data retention. The stakeholder groups' views on this issue reflect stakeholder beliefs about the appropriate collection, use, access or disclosure of personal health information. In general, those who believe that individuals have the ultimate right to protect their personal privacy also firmly believe that, in most circumstances, explicit consent is required for personal health information to be collected, used, or accessed. Those who believe that the benefits to society of permitting broader access to personal information generally suggest that explicit consent is not always necessary, nor reasonable or practical.

However, the health community is not as divided on this issue as it may first appear. To the contrary: all of the stakeholder groups considered for this study agree that one must obtain consent before collecting, using, accessing, or disclosing individuals' personal health information.

There are a few limited, practical exceptions to this rule. While, generally, nonconsensual collection, use, access or disclosure of personal health information is perceived to be an ethical violation, the Canadian Medical Association (CMA) and the Consumers' Association of Canada (CAC) suggest that it may occur only when required by law, when ordered by a court of law, or in emergency situations. CAC also suggests that an exception can be made when requiring consent "would put the consumer or others at grave risk."[50]

The BC Freedom of Information and Privacy Association (BCFIPA) supports only part of this fourth exception. The Association has not found any evidence to support the notion that accessing one's own information can cause harm to oneself; however, BCFIPA recognizes that in certain very limited circumstances an exception may be justified. As expressed by Darrell Evans, BCFIPA's Executive Director, "in these circumstances there

[48] *Supra* 159(80), p.1005.
[49] Consumers' Association of Canada, *Supra* note 44, p. 6, section 8 safeguards.
[50] Consumers' Association of Canada, *Supra* note 44, p. 5, section 5.

is a very high onus on the decision-maker to show there is a probability of harm to another – for example, overt threats or a history of violence."[51]

The Public Interest Advocacy Centre (PIAC) submits that there may be narrow exceptions where the requirement to obtain consent may be overridden; however, the Centre has not yet debated or outlined what these exceptions might be. The Privacy Working Group also recognizes that there may be extraordinary circumstances that demand the use of personal health information without an individual's consent. The Group allows for an exception where there is "a demonstrated legal requirement; or compelling evidence for individual or societal good and a privacy impact assessment that are adjudicated by an independent body according to strict protocols."[52]

Setting these varied exceptions aside, it is quite clear that the community insists that consent is needed for purposes that involve personal health information. Where this black and white issue shows many shades of gray is in determining whether or not consent needs to be overtly demonstrated before collecting, using, or accessing personal health information for primary and secondary purposes. The stakeholder groups take one of three discrete positions on this issue.

The first group requires that, by default, explicit consent be sought. This position only allows consent to be implied for limited and clearly articulated circumstances. PIAC is among the stakeholder groups that take this point of view. The Centre believes that there is a need to justify why an exception is warranted. BCFIPA can also be counted among the supporters of this position. The Association does not see why informed consent cannot be obtained in the therapeutic context and, moreover, is "not convinced that it is right or necessary to use personalized information for research without consent."[53]

A second group of stakeholder organizations broadly and separately acknowledge the circumstances whereby either explicit or implied consent is acceptable and practical. The Privacy Working Group took this approach in its deliberations, as expressed through the draft Principles for the Privacy Protection of Personal Health Information. The Group offered definitions of explicit and implied consent yet only used the term implied consent in one instance; the Group agreed that consent could be implied to provide individual care or prevent harm. The term 'explicit consent' was not used at all, though might itself be inferred in interpreting the draft principles.

The Canadian Medical Association (CMA) and the Consumers' Association of Canada also fit into this group of stakeholder organizations but their positions are more specific than that of the Privacy Working Group. The CMA dedicates one of its ten principles to the concept of consent. Each sub-clause details specific situations where express consent is

[51] Personal communication by e-mail from Darrell Evans, January 31, 2002.
[52] Principles for the privacy protection of personal health information, p. 6, section 3.3 iii b.
[53] *Supra* note 43

required or may be inferred, or qualifies the circumstances under which a patient may grant, refuse, or withdraw consent. An excerpt from the introductory paragraph of the consent principle summarizes CMA's position on this issue:

> "The patient's ability to decide with whom he or she will share information is crucial for the protection of the right of privacy and for the preservation of trust in the therapeutic context. Only the patient's consent to health information collection, use, disclosure and access for the primary therapeutic purpose can be inferred. Except for the very limited nonconsensual purposes addressed in this Code, any other collection, use, disclosure or access requires express consent. Nonconsensual collection, use, disclosure or access infringes the right of privacy and compromises the trust of the fiduciary relationship."[54]

The CMA further notes that the proposed collection, use, disclosure, or access of health information for legislated or non-legislated secondary purposes must first be subjected to a test. Secondary purposes are divided into two categories. Legislated secondary purposes include health information collection, use, disclosure or access required or permitted by legislation or regulation. Non-legislated secondary purposes include, for example, education or research not governed by legislation.[55] The test for legislated secondary purposes is separate from the test for non-legislated secondary purposes. However, both tests require that the proposed purposes be subject to a patient privacy impact analysis before proceeding.

The Consumers' Association of Canada (CAC) takes a similar stance to the CMA; explicit consent is always required, except for therapeutic purposes. In such cases, consent may be implied. CAC requires that explicit consent be in writing where personal health information is to be collected, used, or accessed for secondary purposes.[56] This includes research.

Researcher organizations represent the third group of stakeholders who stand divided from others on the issue of explicit consent. Unlike CMA and CAC, the Canadian Institutes of Health Research (CIHR) does not take a position on the use of personal health information for primary therapeutic purposes. This can be easily explained; the organization primarily speaks for those who have research interests. The researchers also do not outline circumstances whereby consent may be implied. Instead, the agency stipulates circumstances whereby the need to demonstrate explicit consent stands or can be reasonably overridden.

[54] Canadian Medical Association, *Supra* note 39, 1003, excerpt from intro to Principle 5.
[55] Canadian Medical Association, *Supra* note 39, 1001, clause 3.1 (b)
[56] Consumers' Association of Canada, *Supra* note 44, 4.

Where humans are directly involved as research subjects in clinical research studies, CIHR's position is clear: explicit informed consent must be obtained before subjects will be included in research studies. Medical research involving human subjects is governed by the Tri-Council Policy Statement: *Ethical Conduct for Research Involving Humans*. The statement requires that research be reviewed and approved by a research ethics board (REB). The policy statement requires that all prospective subjects be given the opportunity to give free and informed consent before and while participating in the research. In some cases, consent for research purposes can be directly tied to consent for primary purposes. For example, a cancer patient who is participating in a drug trial is simultaneously contributing to a research study and receiving care.

Where personal health data has already been collected for another purpose, though, CIHR argues that it is not practical to seek explicit consent to use the data for secondary research purposes. Moreover, the Institutes suggest that doing so can be self-defeating. CIHR identifies several factors to back up its arguments. These factors include:

> "the sheer size of the populations studied; the wide range of relevant information examined; the age of the data; the significant number of persons who may have since relocated or died; the risk of introducing potential bias through the consent procedure itself thereby affecting the generalizability and validity of research results; the creation of even greater privacy risks by having to link otherwise de-identified data with nominal identifiers in order to communicate with individuals so as to seek their consent; the lack of any real opportunity for direct contact between the researcher and each individual in the study population; and, the practical difficulty of involving the original data holders to establish contact on researchers' behalf."[57]

On the one hand, it seems that CIHR supports the need to obtain and demonstrate consent for personal information to be used for research purposes. On the other hand, CIHR claims that it is often impractical to obtain such consent and research should nevertheless proceed. It appears initially that this position would conflict with the research ethics guidelines CIHR endorses. However, the policy statement allows for the consent requirement to be overridden in defined situations. As noted in Article 2.1 (c), research ethics boards may "waive the requirement to obtain informed consent, provided that the REB finds and documents that:

i. the research involves no more than minimal risk to the subjects;

ii. the waiver or alteration is unlikely to adversely affect the rights and welfare of the subjects;

[57] Canadian Institutes of Health Research, *Supra* note 46, 11.

iii. the research could not practicably be carried out without the waiver alteration;

iv. whenever possible and appropriate, the subjects will be provided with additional pertinent information after participation; and

v. the waivered or altered consent does not involve a therapeutic intervention."[58]

The research ethics boards are mandated to take a number of considerations into account before deciding whether or not to waive the requirement to obtain informed consent to collect, use, or access identifiable personal information. As noted in Article 3.2 of the Tri-Council Policy Statement, these considerations include:

(a) "The type of data to be collected;

(b) The purpose for which the data will be used;

(c) Limits on the use, disclosure and retention of the data;

(d) Appropriate safeguards for security and confidentiality;

(e) Any modes of observation (e.g., photographs or videos) or access to information (e.g., sound recordings) in the research that allow identification of particular subjects;

(f) Any anticipated secondary uses of identifiable data from the research;

(g) Any anticipated linkage of data gathered in the research with other data about subjects, whether those data are contained in public or personal records; and

(h) Provisions for confidentiality of data resulting from the research."[59]

There are, however, no directives as to the constitution of the research ethics boards, or their independence, transparency or accountability.

To summarize, stakeholder groups agree that, in theory, one must ensure consent before collecting, using, or accessing personal health information for primary or secondary purposes. Stakeholder groups disagree on the circumstances where consent must be explicit, where consent may be implied, and when and if the need to demonstrate consent may be overridden.

[58] Medical Research Council of Canada, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, *Supra* note 41, 2.1.
[59] Medical Research Council of Canada, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, *Supra* note 41, 3.3, Article 3.2.

3.5 Consent to disclose personal health information

The stakeholder groups are less divided regarding disclosure requirements. Where the groups allow personal health information to be collected, used, or accessed by consent for primary purposes, the same holds true for disclosure of this information. Further, where groups stipulate that explicit consent needs to be assured to collect, use, or access personal health information for secondary purposes, the groups agree that this stipulation extends to disclosure of information.

For example, the research community justifies circumstances where research ethics boards have the authority to override the need for researchers to demonstrate that consent has been obtained to collect, use, or access personal health information. In this regard, CIHR's position stands in stark contrast to the positions taken by the other stakeholder groups. The Institutes' position on disclosure restrictions, however, is indeed closely aligned with the rest of the health community:

> "information that is disclosed in the context of a professional or research relationship must be held confidential. Thus, when a research subject confides personal information to a researcher, the researcher has a duty not to share the information with others without the subject's free and informed consent. Breaches of confidentiality may cause harm: to the trust relationship between the researcher and the research subject; to other individuals or groups; and/or to the reputation of the research community. Confidentiality applies to information obtained directly from subjects or from other researchers or organizations that have a legal obligation to maintain personal records confidential."[60]

There is therefore a general agreement among stakeholder groups that the principle of confidentiality is not to be trod upon lightly with regards to disclosure of personal health information.

3.6 Health research purposes

Thus far, secondary purposes have generally been discussed as a whole. There are a few additional noteworthy discussion points about a subset of secondary purposes, namely health research, that help to further illustrate the wide-ranging questions to be answered in the broader debate.

Stakeholder groups, for the most part, purport that there is a need to balance individual privacy rights with data access rules that permit research to be conducted for the good of society. The question is: who should decide which research purposes are of such societal benefit that they outweigh any risks of infringing on individuals' privacy and confidentiality

[60] Medical Research Council of Canada, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, *Supra* note 41, 3.1.

rights? And further, if there is any doubt as to whether explicit consent must be sought to collect, use, access or disclose personal health information, who should have the ultimate authority to make this decision and to oversee the process? When it is decided that access to personal health information should be granted for secondary purposes, through whom should individuals exercise their right to have this decision reviewed or to file a complaint? There is no agreement on these issues amongst the stakeholder groups reviewed.

3.7 Patient access to records

Another area where there is general agreement in theory, but there are few accepted standards in practice, is in the context of patient access to records containing personal health information and redress procedures. The stakeholder groups generally support the following concepts:

- There should be a process for patients to follow to access records containing personal health information;
- The access process should be open and transparent;
- Patients should be able to obtain a copy of records containing their personal health information for free or for a reasonably minimal charge;
- Patients should be able to ask a knowledgeable health professional for help in interpreting records containing personal health information; and,
- Patients should be able to determine who has previously accessed their personal health information.

There are only two exceptions. First, the Consumers' Association of Canada does not state specifically that patients should be able to obtain a copy of their records. It does, however, emphatically state that consumers should have access to their health information so that they may review the information and ensure any necessary corrections are made. Second, from the literature reviewed about the Canadian Institutes of Health Research's (CIHR's) health privacy positions, it is unclear whether or not CIHR takes a position on this issue at all.

There is no discussion from the stakeholder groups' documents about what could be considered the ownership of patient records. Some advocates have expressed the belief the recognition of individuals' rights over information about themselves should entail the ability for patients to move their records from physician to physician rather than just have the ability to access, copy or correct the information in it.

3.8 Data integrity and redress provisions

Similarly, stakeholder groups generally agree on the following redress provisions:

- There should be a process for patients to follow to correct records containing personal health information;

- The correction process should be open and transparent;
- Patients should be able to appeal decisions when they are denied access to see or to correct records containing personal health information;
- There should be penalties imposed on those who collect, access, use, or disclose personal health information when it is inappropriate to do so; and,
- Patients should be able to seek and obtain compensation when they have suffered as a result of others' inappropriate collection, access, use, or disclosure of their personal health information.

There are only a few exceptions to be noted here. Again, it is not clear from the literature provided by CIHR whether or not the research community has taken a position on the redress issue. And further, only the Public Interest Advocacy Centre and the BC Freedom of Information and Privacy Association have addressed the concepts of penalties and restitution. These two organizations believe that individuals should be compensated when they have suffered as a result of a privacy violation, but neither organization has yet debated what compensation would be appropriate.

4 Research on Consumer Views

Canadian consumer views on the issue of the privacy of personal health information, elicited either through an email survey or in person through focus group discussions, are presented below in the context of the broad issues defined in sections one and three. Some issues raised by consumers go beyond those addressed by stakeholder groups or in the legislation and even within the scope of issues common to all three there are clear differences in emphasis.

Data reported are from three sources: focus group discussions, focus group summary surveys and email/mail-in surveys. As noted in section 2.3, results from the focus group summary surveys and email/mail-in questionnaires, which asked the same questions, have been presented as a whole, except where there were significant differences between the two groups. These are noted and addressed where appropriate. Sample size was insufficient to report meaningful demographic differences (age and gender).

4.1 What do privacy and personal health information mean to the consumer?

4.1.1 Privacy

Given the clear definitional problems identified in sections two and three, focus group participants were asked at the outset what privacy meant to them in a general sense and in the context of personal health information (personal health information). The key word that emerged in all five groups was control. Privacy was seen to centre around the ability to control access to one's information and how that information is used, supporting the definition proposed above in section 1.3. A number of participants in different groups noted that for privacy to be real, control over the information had to be ongoing. Personal health information must be seen to remain under the control of the individual to whom it belongs, otherwise that individual has no guarantee of privacy.

There was little discussion in terms of a consumer's right to privacy in that this seemed to be taken as a given, although in the Ontario group particularly there was skepticism regarding the extent to which one might really expect privacy in today's information world. Several participants in different groups also noted a point at which the right to privacy may need to be set aside. Examples were given regarding the sharing of information to protect society, such as in the case of communicable diseases, medical conditions which affect driving ability and the point was made that in some professions, for example teaching or in the handling of prisoners, certain health information regarding potential problems is required to properly perform one's duties. For the most part there was little disagreement regarding the need to suspend privacy in such cases, although it was noted that these are relatively few in number, implying that they can be quantified and clearly identified as exceptions. In

Alberta there was extensive discussion of the issue of privacy in the workplace with two opposing views. The first, similar to that expressed in other groups, was that in certain cases privacy may need to be suspended, but if information is released employers should be subject to the same duty of confidentiality as doctors. The opposing view was that employees should never be required to provide personal health information to employers; the responsibility to remove oneself from employment when unfit physically or psychologically should be left with the employee. This was a uniquely Albertan view.

One participant in the Quebec focus group noted that privacy does not appear currently to be treated as a right, citing the common marketing practice of asking individuals to check a box if they do ***not*** wish their information to be shared with other companies. In his view this implied the norm is indeed to share such information.

4.1.2 Personal health information

Among focus group participants, personal health information was generally understood to refer to medical records, including doctor's opinions, comments, diagnoses of physical and psychological illnesses and medications related to those illnesses, or in other words, information stemming from the doctor-patient relationship. The two Ontario groups went somewhat further including insurance-related information, school reports and workplace-related health reports, as well as lifestyle information. Demographic information was also mentioned in two groups in the sense that membership in a particular demographic can be extrapolated to reflect certain health issues.

4.2 Awareness and importance of privacy and personal health information

Focus group participants on the whole felt they were not very aware of this issue before participating in the discussion. When asked to rate on a scale of 1 - 10 their level of awareness[61], they indicated a mean rating of 4.76 (SD 2.2), with a range of 1 - 8. The distribution, however, was bimodal reflecting two sub-groups. One slightly smaller sub-group was relatively aware (7,8) while participants in the other, larger sub-group rated themselves as largely unaware (2,3,4). There was no significant difference from province to province in self-attributed awareness. As one participant in the Ontario group commented, this is the sort of issue you probably do not think about until something happens to you. Indeed a number of participants who had experienced some problem in the handling of their personal health information appeared much more aware of the issue and the potential consequences of problems in this area. Many noted in their final comments on the survey that they would think about the privacy of their personal health information much more in the future now that they had been made aware of the issue. Few mentioned having seen

[61] Where 1 indicated no awareness and 10 indicated total awareness of the issues discussed.

anything in the press and it was suggested in one group that the issue is not very politically salient and hence tends to be ignored.

Survey respondents were asked to rate on a scale of 0 - 5 to what extent they were satisfied[62] with the amount and quality of information they had received from any source to date regarding this issue. Mail-in/email respondents who had not been exposed to information in the focus groups indicated they were not very satisfied (average rating 1.98 (SD 1.42) for quantity and 2.00 (SD 1.45) for quality). Focus group participants, perhaps including in their rating the information provided in the two-hour discussion, indicated they were significantly more satisfied than the mail-in/email group, but still only moderately satisfied (average rating 2.68 (SD 1.43) for the quantity of information and 2.86 (SD 1.45) for the quality of information). These data support a point made several times during the course of the focus group discussions to the effect that there is a clear and pressing need for greater public education on privacy and personal health information.

4.3 Consent

In each focus group approximately one half of the participants indicated that they routinely do not read consent forms, or for those who could not remember a specific experience, they considered they would be unlikely to do so unless for a very major or risky procedure. The unique context of signing a medical consent form for treatment was noted, in which the worry and sometimes the urgency of treatment means the patient's attention is elsewhere. Furthermore in several groups mention was made of the inherent trust in doctors and the medical profession, instilled from an early age, which may suggest a close reading is not necessary. As one member of the Francophone group noted, though, we do not consider signing bank forms without closely reading them, so why do we do so with medical forms? The extent to which trust in the medical profession is warranted was a matter of some debate, with some suggesting certain individuals do not inspire much confidence. Others were of the opinion that medical professionals work under a strict code of ethics and deserve our trust.

4.3.1 Awareness of consent issues

In four of the five focus groups there was little awareness that signing a form for treatment implied giving permission to health care providers to disclose information for secondary purposes. Many individuals thought that separate consent forms were necessary or, as a Manitoba participant noted, that if such information were divulged, it would only ever be in de-identified format. Only in Alberta were at least half the participants aware that they were consenting to the release of their information. This may reflect a greater sensitization in Alberta to the privacy and health information debate in the wake of the recent enactment of provincial legislation in this regard (see section 5).

[62] Where 0 means not satisfied at all and 5 indicates a great deal of satisfaction (see appendix C.2)

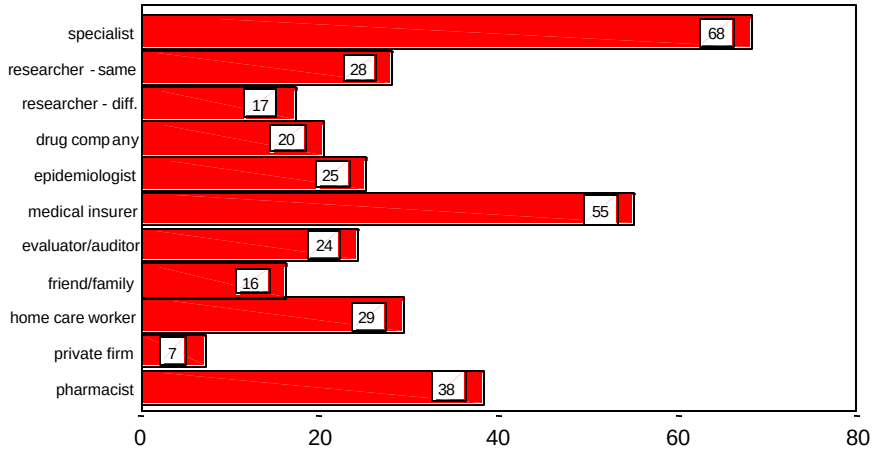
One issue raised consistently throughout the focus group discussions was the problem of readability and simplicity in consent forms. Many felt they could not easily understand what they were signing given the complex language and the length of such forms, so they could not be expected to be aware of what was included in the consent when it was not set out clearly. As an Alberta participant questioned, is it really informed consent if I don't know how my information will be used?

In the survey, respondents were asked to indicate who they believed currently could access their identified personal health information without consent. If this sample is representative, consumers do not seem to be very sure about the current practices surrounding access to personal health information. Figure 4.3.1.[63] shows the number of respondents who thought which among eleven entities could access their personal health

Figure 4.3.1

Who can access my PHI?

(77 responses)



information with no formal (or informal) consent. There was general (although not unanimous) agreement that specialists and medical insurers likely could, while private firms generally could not, but there was considerable disagreement as to the rest. What is not evident in the graph, but reflective of widely varying views on the status quo, is that some individuals believed that just about anybody could access their personal health information, while others thought almost no one could.

[63] Researcher-same refers to a researcher studying the same disease or illness as the patient whose personal health information is in question; researcher-diff. refers to a researcher studying a different illness. See Appendix C.2 for specific questions or table 4.4.1.1 for more complete phrasing.

4.3.2 The importance of consent

In the focus group discussions, there was strong agreement that consent is an important issue, which is at the heart of the concept of privacy, which, as noted above, centred for most participants on controlling the use of information. Fear was expressed regarding the consequences of the promulgation of information that may be inaccurate. One participant put forward the idea that the only way to avoid this was to be in control and personally responsible for the release of information.

Also important for these consumers was their right to freely withhold consent (with no penalty) for secondary use of their personal health information. Several groups mentioned the very difficult situation a patient faces when asked to sign consent for treatment, if unwilling to have personal health information released. Given the frequent linking of the two in the same form, participants believed it very likely that the patient would feel he/she had no real choice. Patients must sign to receive treatment, so how can they refuse? Very few were aware that they could modify the form if there was anything they wished to see stated differently or that they could add anything they felt was missing. Again the trust in medical professionals was stressed, although some suggested that such trust may be inappropriately extended to all in the health care profession (office staff, hospital staff, etc.).

When asked on a scale of 0 - 5[64] to what extent survey respondents feared that restricting access to personal health information may negatively affect the delivery of health care, the mean response among focus group participants was 3.53 (SD 1.2), suggesting this is a real concern for patients. They may wish to withhold information, but may feel unwilling to jeopardize their immediate treatment or perhaps even subsequent contact with the health care system by clearly stating as much. Although significantly less concerned than those in the focus group, mail-in/email respondents were also somewhat concerned about this, with an average response of 2.79 (SD 1.72). The higher levels of worry among focus group participants may reflect the fact they had had time to consider some of the implications of restricted access over the course of the discussion.

[64] Where 0 reflects no concern with the issue and 5 a great deal of concern.

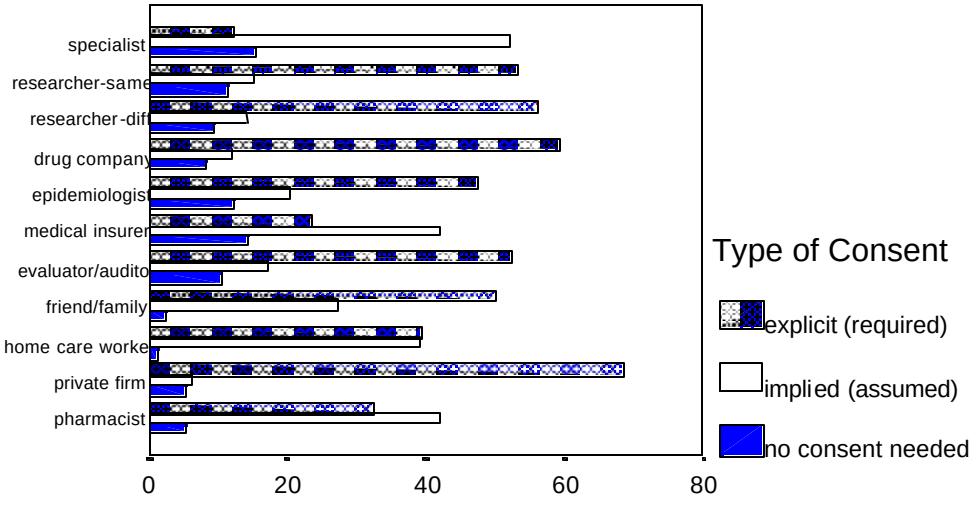
4.3.3 What aspects of consent are central to consumers?

The major difference between the stakeholder group and consumer view of consent was with regard to the distinction between implied and explicit (or express) consent. Although the definition of these two types of consent was provided to focus group participants and survey respondents (by way of examples) both sets of respondents appeared much less concerned about this distinction than that between identified personal health information

Figure 4.3.3.1

Type of Consent Currently Required

(77 responses)



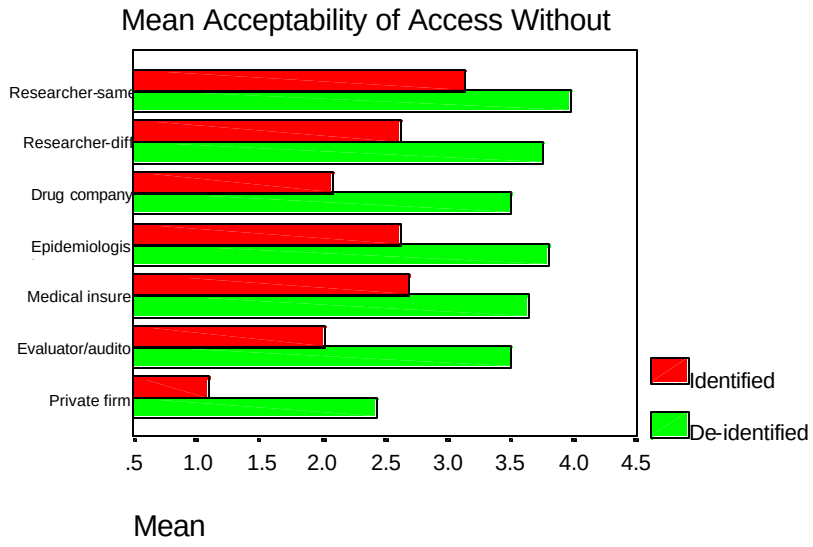
and de-identified personal health information.

Figure 4.3.3.1 indicates who respondents believed currently requires explicit, implied or no consent to access their personal health information. Most believed that all the entities save three required explicit consent. The three exceptions were a specialist called in to help on the case, the medical insurer and the pharmacist. In other words, exceptions applied to entities who respondents felt were intimately related to the provision of their primary care. The choice of explicit or implied consent by user varied widely among participants and, as figure 4.3.3.1 shows, each of the three options was chosen by at least some respondents in each case. Examining the patterns of response, there appears to be a meaningful difference between explicit (express) consent and implied/no consent, but the latter two were often confounded.

Many respondents chose to contrast explicit consent with implied consent, while others contrasted it with no consent. A few used all three, but not with any clear pattern. For most consumers it appeared that **consent means clearly stated consent, not someone else's view of what you probably would consent to, if asked**. As one Manitoban participant suggested, implied consent is simply too vulnerable to abuse, so it is really little different from no consent. This is clearly a very different perception than that prevalent among the stakeholder groups, who make a clear distinction between implied consent and no consent. This difference in view between a dichotomous consumer perspective and a more finely differentiated stakeholder group perspective is a potential source of confusion and misunderstanding, which must be considered in engaging the consumers in the debate.

On the other hand, when asked how comfortable they would be with having their personal health information released with identifying information and without identifying information to various potential users, participants made a clear and definitive statement. In all cases[65] they were

Figure 4.3.3.2
Identified vs. De-identified PHI



statistically significantly more concerned about the release of identified rather than de-identified information (see Figure 4.3.3.2)[66].

All focus group participants were made aware of recent findings that show that de-identified information can sometimes be re-identified given frequent linkages among

[65] Note that only personal health information for secondary use was contrasted here, since it makes little sense to talk of releasing de-identified information to a home care worker or specialist called in on the case.

[66] Given the number of tests conducted, statistical significance was set at a conservative $p < .001$ (the probability that the result is by chance is less than 1 in 1000).

databases. While this was definitely a subject of concern, many participants felt there was not much that could be done to prevent this and, realistically, it was probably not that likely to happen, given the effort involved. Since the distinction between identified and de-identified information was so evident in the responses of consumers, it is clear that consumers expect de-identification to be conducted thoroughly and consistently when needed and to a degree that minimizes the possibility of re-identification. Once de-identified, though, there is a much greater willingness to share information for most secondary purposes, with the notable exception of commercial gain.

Another issue specific to the Alberta group was concern over the presentation of a health card as a proxy for consent to disclose information. Focus group participants felt strongly that showing such a card should not be construed as consenting to any release of personal health information. The focus on this issue may again reflect a higher sensitization to privacy issues among Albertans as a result of the enactment of recent legislation.

4.3.4 Consumer solutions to the debate over consent

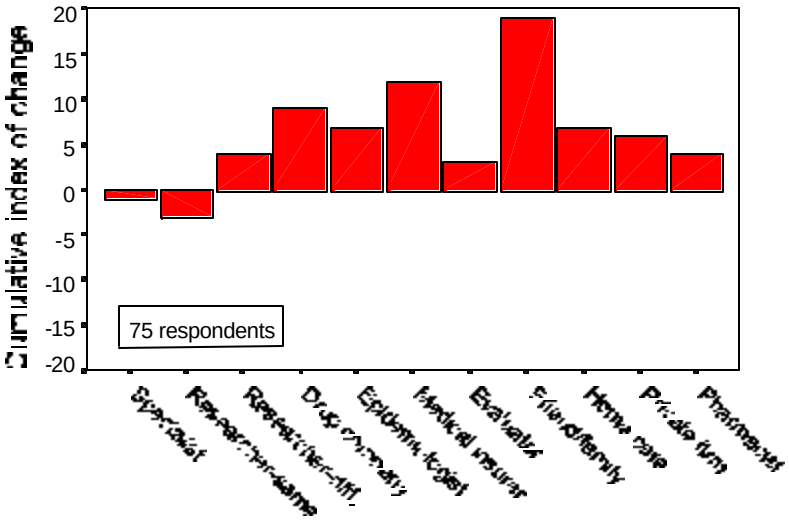
Across the focus groups, perhaps the single most frequent recommendation in this regard was the need to simplify and streamline the process of consent while at the same time introducing more control for the individual. There was strong agreement that treatment consent and the consent to use personal health information for secondary purposes should be separated, ideally set out on different forms. Many participants were also of the view that they should have the right to indicate consent each and every time their personal health information is used, although there was widespread recognition that it was simply not feasible to ask for written consent every time any of their information was going to be used for any purpose.

In many ways the recommendation emerging in some groups was reminiscent of that of the BC Freedom of Information and Privacy Association's layered consent. In one group a sort of donor-card like system was put forward in which each individual would set out which (secondary) uses of his or her personal health information were acceptable. The caveat was that this list may need revising from time to time as the nature and extent of the individual's personal health information changes. In another group, a similar process was suggested, but was directed more at the primary health care provider (often the family doctor) who would at the initial intake note the wishes of the consumer and thereafter on occasion offer him or her the opportunity to update the list of choices. Clearly this puts a heavy administrative burden on an already over-taxed portion of the health care system. At the very least, consumers felt they should be notified if their personal health information were to be used for purposes other than those discussed in the original consent.

Figure 4.3.4

More or less explicit consent?

(positive values = more stringent consent)



In comparing the items on the survey that asked what sort of consent is currently needed and what sort of consent should be required, we find a general trend towards greater (explicit) consent over implied or no consent. In Figure 4.3.4 the 0 axis represents no change required, with negative values reflecting a desire for less rigorous consent (i.e., a shift from explicit to implied/no consent) and positive values reflecting a desire for more rigorous consent (that is, a move from no consent/implied consent to explicit consent). Only in the cases of a specialist called in to help on the case or a researcher researching the same illness as the patient, was there a slight shift towards requiring lower consent. In all other cases, the desire across participants was for more stringent consent. It is very important to note, however, that this desire for change (reflected in the ratings to the left on the graph) is cumulative, so that only between 20 to 40% of those sampled desired any change at all. In other words, in each case the clear majority of respondents did not indicate any need for a change to the status quo. This in turn must be considered in light of the fact that many respondents clearly indicated they really didn't know what the current situation was. There may well have been a much greater desire for change if participants had been given a clear picture of the status quo[67].

[67] This was not done as one of the primary purposes of this research was to ascertain what is the current level of awareness regarding issues such as consent (see section 2.3)

4.4 Access to and disclosure of personal health information

Discussion and survey responses on this issue were again sought to clarify what consumers think is currently the practice and if and how they would like to see that practice changed.

4.4.1 Awareness of current practices

In the focus groups, there was no clear perception of exactly who could or could not currently access personal health information without consent, although it was thought that de-identified personal health information could be much more easily accessed than identified personal health information. As well as primary health care workers, focus group participants named insurance companies, employers, schools (in certain cases), government agencies, banks, commercial entities, and others as potentially able to access identified personal health information. When the handout listing those who might be interested in accessing personal health information was given out (see Appendix C.1), several participants in various groups were astonished at the range of entities involved. Indeed, in two groups, Ontario and Alberta, the comment was made that everyone seems to have access except the individual involved.

In the survey data, a slightly clearer picture emerged, with the majority of respondents considering that specialists, insurers and pharmacists are able to access identified personal health information without consent, but other entities require consent. As noted above in section 4.3.3., however, this view is far from unanimous. In table 4.4.1.1 the percentage of respondents who thought the entity listed could access their identified personal health information without consent is set out by source of data.

Table 4.4.1.1
Currently, who can access your personal health information without your consent?

Entity	**Percentage of participants who think identified personal health information can be accessed by this entity without consent**		
	Focus Group (36 responses)	Mail-in/Email Survey (42 responses)	Total (78 responses)
Specialist	83%	93%	88%
the insurer for the medical procedure involved	75%	69%	71%
Pharmacist	53%	48%	49%
a home care worker who is to work with the patient	47%	31%	38%
Researcher researching the same illness as patient	39%	36%	36%

Entity	Percentage of participants who think identified personal health information can be accessed by this entity without consent		
Epidemiologist	36%	31%	33%
a health care system evaluator or auditor	42%	24%	31%
drug company researching new drugs	39%	17%	26%
Researcher researching a different illness than patient	31%	17%	22%
a family member	28%	14%	21%
a commercial entity	19%	0%	9%

Perhaps most striking in these numbers is that between 10 to 40% of respondents actually believe that many individuals can access their personal health information without consent for secondary purposes, certainly a far cry from a solid sense of privacy. When asked directly how well they thought the privacy of their personal health information was being protected, the response was overwhelmingly not well at all (see section 4.7.2 below).

4.4.2 Who should be able to access my personal health information?

When asked to indicate on a scale of 0 - 5 how concerned they were about the possibility that individuals may be permitted access to their personal health information without permission, survey respondents and focus group participants indicated a relatively high level of concern (mean rating 3.6, SD 1.4). They were also concerned that their personal health information may be used without their permission for purposes other than their primary care (mean rating 3.5 SD 1.5).

It was also clear that consumers have different comfort levels with regard to who should be allowed access to their personal health information and for what purpose[68]. In rank order from the highest "comfort-level" to the lowest in terms of sharing identified personal health information were:

- a specialist called in to help on the case
- researcher studying the illness of the patient in question
- pharmacist
- insurer
- researcher studying an illness other than the one the patient has
- researcher studying the prevalence of the particular illness (epidemiology)
- home care worker assigned to help the patient recover

[68] $F_{(10)} = 24.82$, $p < .001$ in a repeated measures analysis of variance.

- drug company researching new drugs
- health care system (program) evaluator
- friend or family of the patient who may be able to support the patient
- commercial firm selling products of potential interest

Differences among the users that were statistically significant included primarily a much greater comfort level with specialist access and much lower comfort level with private firm access than virtually all other potential users[69]. In general, though, the quantitative data support the sense that emerged from the focus group discussions that direct delivery of health care is generally thought to require fairly ready access to personal health information, while purposes associated with potential financial gain are the least acceptable (commercial firm and drug company). The lack of willingness to share personal health information with family or friends reflects perhaps the stronger threat to privacy inherent in those close to you knowing so much. As one participant mentioned, though, this is likely very case specific in that it may well depend on how sick and/or competent one is as a result of the illness in question.

Participants in several focus groups made the point that sometimes information that needs to be shared (for instance tests or a patient's medical history when moving) is not shared between medical professionals resulting in delays and extra cost to the system. This was not specifically blamed on privacy, but rather used as an example of how the flow of information to those who need it to care for the patient is important. This echoes the concern mentioned in 4.3.2, in which there was a clear fear that a lack of information could hurt the delivery of primary services.

4.4.3 To disclose or not to disclose? Overview and consumer suggestions

In weighing the implications of greater control over personal health information (maximum privacy) or wider access to personal health information (blanket consent), most focus group participants recognized several advantages to either stance. Among the advantages of open access to personal health information, the following were noted (numbers after the bullets reflect how many focus groups mentioned the issue, from a minimum of one to a maximum of five):

w (5) **improved research ability**, leading to quicker and more effective cures. Society would also be able to have greater confidence in the research conducted given that numbers would be higher and there would be comprehensive access to the data required (rather than proxy or incomplete data). Statistics collected would be more comprehensive and could therefore be relied on to develop more successful treatments.

[69] Various other statistically significant differences between different pairs of users were also found, but are not included here in the interests of clarity.

w (4) **improved health care delivery** as a result of a streamlined information management system, allowing timely access to relevant information. The onerous paper-trail implied in tracking consents for various purposes would not be needed, allowing scarce health care dollars to be spent on what is most important, primary health care.

w (2) **improved safety** as a result of good cross-referenced databases. This would include the ability of the system to track counter-indicated drug use (from different sources) or to identify more easily patients who unknowingly may be a threat to themselves or society as a result of piecemeal or fragmented health care, e.g. the paranoid schizophrenic patient who stops filling his prescription.

w (2) **better information on products of potential interest** as a result of marketing firms knowing what is relevant to you. In Manitoba, the point was made that if a drug company knows that you suffer from illness x, it may contact you directly with relevant information and alternatives, including alternatives possibly not suggested by your doctor. For the most part, though, this was not seen to be a particularly strong advantage, given the link to commercial profit. As one participant noted, the driving force is not the benefit to the patient, but profit to the company, so it is hard to trust such information. The Consumers Association of Canada has steadfastly argued against direct drug advertising to consumers for this and other reasons.

w (1) **additional funds for hospitals** through the selling of patient lists to firms for marketing purposes. While recognized as an advantage to the hospital there was almost unanimous agreement that such a practice would not be good for patients and should be avoided at all cost.

w (1) **better extra-medical delivery of services,** resulting from an awareness of conditions that may impact behaviour at school or work. In other words, if educators or employers were aware of specific conditions they may be able to intervene more appropriately, tailoring the work or school situation to better suit the individual. This point was endorsed by the Francophone group, in which several of the participants were involved in teaching or day care.

w (1) **access to clinical trials, potential treatments** which might only be available if the organization running the trials can access easily who has what condition. In other words, having a clear picture of who is suffering from what may open doors to wider treatment options.

w (1) **availability of potentially lifesaving information** with no protracted court battles. The example here, raised by the Manitoba group, was in regard to adoptive children and their birth parents. Children could easily and quickly obtain relevant genetic and medical histories of their parents. This was equally true for any estranged relative.

However the opposite end of the scale, in which the individual controls all access to his or her personal health information, was also seen to offer many advantages:

- (4) **less likelihood of harmful information being released to the wrong parties.** For many participants this was the major advantage of greater personal control, particularly given the potential damage that could be caused by the release of inaccurate information. Many participants considered one of the major disadvantages of widespread access to personal health information to be the potential for discriminatory practices or "labelling" based on having a particular illness. Stringent personal control of such information would avoid any fear of that information being released.

- (4) **no unwanted marketing pressure** since the information would not be available to commercial entities unless specifically given by the individual. This was seen as a major advantage by most given the widespread condemnation of using personal health information for profit.

- (2) **avoidance of embarrassment or pain,** which may result from unwarranted access to personal health information. The scenario used in the focus group involving a couple who had miscarried and then received baby product advertising shortly afterwards was cited as an example.

- (2) **peace of mind** For some participants one of the biggest advantages was a general sense of peace of mind that they and they alone controlled their information. As one participant in the Ontario group noted, " I am a very private person and worry about others knowing more about me than I am comfortable with".

- (2) **treatment needed will be sought** since those who might otherwise hold back information or avoid seeking treatment at all because of privacy concerns (e.g., HIV) will be able to feel confident their personal health information is under their own control[70].

- (1) **empowerment of patients** Often patients feel very much as if everything is out of their control when they are sick and in the hands of the large health delivery machine. By assuring them control over their information they would feel empowered and accrue some benefit from that sense of personal control.

- (1) **the right to choose** will be safeguarded in that an individual may choose research he or she feels is important and avoid the use of personal health information to support research the individual feels is wrong. The example given in the latter case was embryonic stem cell research.

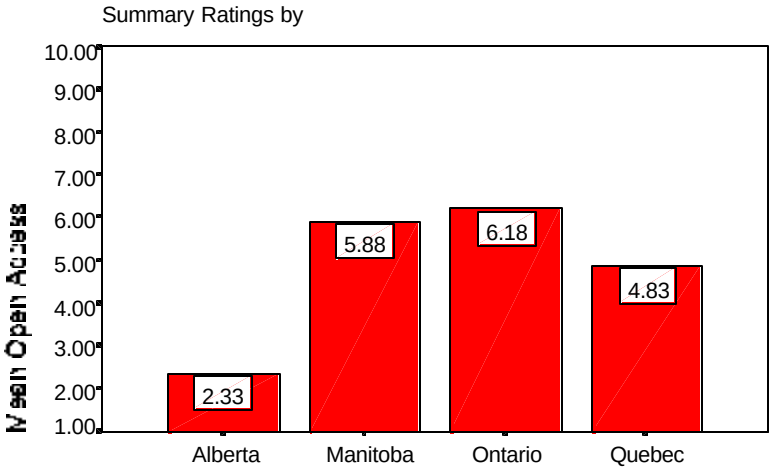
[70] In the survey, respondents were asked if they had ever withheld information because of a fear it would become part of their permanent file. Nine of the 26 respondents who chose to respond to this question indicated they had. Reasons given included information might not have been socially desirable (drugs, drinking), the individual did not want to be "labelled", there was a lack of trust with the professional, or in two cases simply that it was not relevant.

W (1) **protection of civil liberties** would be assured, since information which could be used to circumvent those liberties, such as restricting travel or employment or the provision of insurance would be under the control of the patient. This might be viewed as the positive aspect ("flip side") of the first advantage of greater privacy mentioned above. That is, information will only get to those who need and should have it.

For the most part, focus group participants were clearly aware that there are benefits and (usually diametrically opposed) disadvantages to both extremes. So when faced with the choice, and taking the wide ranging discussion into account, how open (or conversely, how closed) did the four main focus group participants[71] think personal health information should be? Figure 4.4.3 compares the average response by group across the country.

Figure 4.4.3.

How Accessible Should Your PHI be?



Statistically, only the Alberta focus group differed from the others, with Albertan participants indicating they would want significantly more control over their personal health information[72]. This comparison is misleading, however as in all four groups there was a clear divergence of views, with some participants supporting relatively wide open access and others desiring near complete control.

[71] The preparatory focus group was not asked to quantify this choice

[72] $F_{(3,33)} = 3.38, p < .05$

Table 4.4.3
Response Range: Open Access vs. Total Control over personal health information

Group	Low Score	High Score	Standard Deviation
Alberta	1	10	2.9
Manitoba	4	8.5	2.1
Ontario	1	9.5	3.3
Quebec	1	8.5	3

1 = total control over information (no access except with explicit consent); 10 = blanket access with no consent required for access

Table 4.4.3 gives the range of response for each group. In all but the Albertan group, there was a preponderance of individuals favouring greater openness, while in Alberta the reverse was true. In both Ontario and Quebec[73] the comment was made by those participants choosing to support greater access that they would only feel comfortable with a score of 8 or 9, given that they did not support access to personal health information for commercial gain. Several Albertans made the same comment, but chose a rating of 5, suggesting the concern over commercial use of personal health information was seen as a greater overall threat.

In general, then, many participants while recognizing the potential harm in too much access also believed that the benefit to society of more measured access could not be overlooked. Among those who took a more restrictive view many made it clear that having such control did not mean they would not want to give permission to anyone to access their information. Several suggested that research and other secondary uses of personal health information are important. It is just that they wished to have a say in what was done with their personal health information. As one participant among what we might call the "high privacy" group pointed out, it should not be a choice between having control over one's personal health information ***or*** benefitting society. He stated that surely in today's highly technologically advanced world it must be possible to allow people control over their information while at the same time permitting them the choice to support research and other worthy endeavours in a timely and efficient way.

In the Ontario group a number of participants in the "greater openness" group suggested that, given the choice to keep personal health information private or share it, the vast majority of Canadians would probably choose the former, thereby potentially harming society by restricting essential research and oversight. However, participants themselves were surprised that this did not seem to be the case, based on the ratings in that focus group (and in other groups), which tended towards greater openness. If Canadian

[73] The reader is reminded that these terms reflect an Anglophone group, all of whom but one live in Ontario and a Francophone group, all of whom but two live in Quebec.

consumers understand the benefits of allowing access to personal health information then many seem willing to give up a certain level of privacy for that end. One Ontario participant suggested that this reflected the socialist view of medicare: we must give up some individual rights so that all can benefit.

The reader will notice that these results, that is, a tendency to desire greater openness, seem contradictory in light of the results reported in 4.3.4 in which there seemed to be a movement towards greater control over personal health information (explicit consent). The difference may stem from the level at which the question is phrased. In this case we were asking generally how much access should there be to personal health information, while in 4.3.4. the question was contrasting implicit and explicit consent. In general many Canadians, at least many in the focus groups, would like to see a system in which there is greater openness in personal health information for the benefit of society but not for commercial gain. However, when asked to comment on consent in particular cases, respondents were either happy with the status quo or would prefer a more stringent consent arrangement.[74]

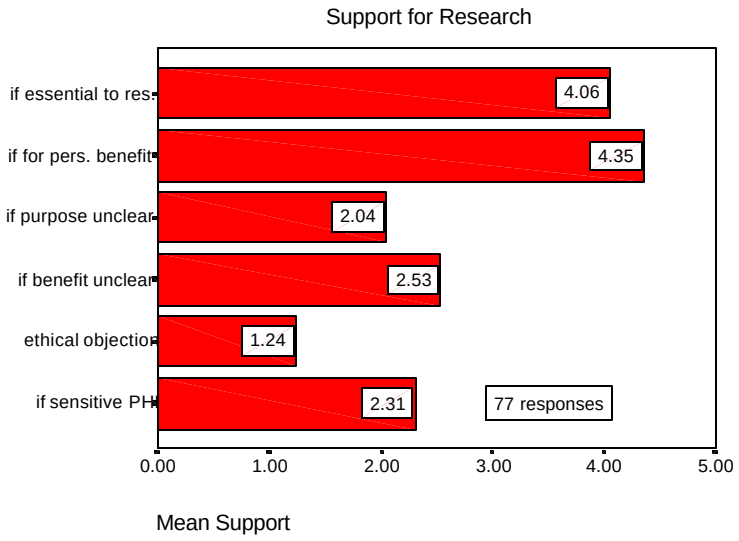
An alternative proposal from one of the middle-of-the-road participants was that we should, as a society, be able to agree upon a clearly demarcated box within which personal health information can be shared freely, such as for primary purposes and some widely supported research, but that outside of which far more stringent measures (explicit consent) are needed to access and use personal health information. In two separate groups (Manitoba and the preparatory focus group in Ottawa), it was suggested that an independent body or panel be set up to determine the value of the project in question so as to grant or not grant access to databases with personal health information. While the issue of Research Ethics Boards (REBs) was not raised directly, the comment was made that any body closely allied with a single organization would be unlikely to inspire confidence in the public. There was some concern among many regarding the ability of any body to be truly "independent".

[74] Initially it was thought this might be a difference attributable to a greater conservatism among mail-in/email survey respondents; however, the composite index of change used in figure 4.4.3. when computed separately for each source, showed that, in fact, focus group participants were more conservative, desiring more change towards more stringent consent than their mail-in/email counterparts.

4.5 Personal health information for research purposes

In the context of both consent and access/disclosure, focus group participants evinced a clear understanding of the importance of research to society and potentially to themselves, should they ever be sick. Among the 77 participants who answered the

Figure 4.5



(res. = research, pers. = personal; see C.1 for specific phrasing)

question in the survey, only 3 (4%) indicated they would not be willing to share their personal health information for research. People were particularly willing to share personal health information if they were convinced their information was necessary for the research and if the research in some way benefited them personally or a friend or family member. Where they were unsure who would benefit from such disclosure, support dropped as it did if the information they were being asked to share was deemed to be particularly sensitive.

Participants were least likely to be willing to share information if they were aware that it would be used in research to which they were ethically opposed. Among other qualifications noted, were the reputation of the researcher and the fact that the research should benefit someone. Several respondents noted they would not want their personal health information used in research that would lead to commercial gain, while another suggested the results of any study she supported would have to be made public. Still others would want assurances about the confidentiality and or anonymity of their data. (see Figure 4.5).

4.6 Access to one's own personal health information

4.6.1 Experiences in accessing personal records

Most focus group participants had never asked to see their own personal health information and while there was some doubt as to whether what they might find would always be accurate, there was a sense that the information would be available if they asked. Twenty participants from among those who completed the survey and answered this question (76) did say that they had had occasion to ask for access and of those, eight (9.5%) indicated they had been refused.

In one case of refusal, the request had been made for a complete medical history upon leaving government service, but the individual was only given a partial file. In four others, the files had been requested to take to a new doctor (or dentist) but the patient had been refused. In two cases the respondent was told that the file was the property of the doctor. This issue is an important one both from an access perspective as discussed by focus group participants, but also in the context of the cost of health care delivery. Many physicians deem test results and x-rays their property and the refusal to release these to patients changing doctors can cost the health care system dearly, given that new, identical tests have to be rerun.

Some participants who had been given access to their files were required to pay for a copy of the file. In a couple of cases the patient refused to pay and thus was forced to "start from scratch" with the new doctor. There was considerable anger at having to pay for information that was thought to be "personal".

For those who had asked to be and had been given access to their file, all but three indicated they had understood what was in the file and, of those, only one said she had received an unsatisfactory clarification from the doctor. The specifics regarding access and clarity of files seems to be a question that requires a much larger sample than the one at hand in order to understand Canadian consumer experiences.

4.6.2 Inaccuracies in personal health information

One of the major reasons participants believed the right to access their personal health information was important was the potential consequence of having inaccurate information in the file. One participant in Ontario had had health insurance refused based on a faulty diagnosis, which was later corrected, but never changed in the medical file. Although he did finally manage to correct the information in that file, he indicated an ongoing concern that the same wrong information might exist in other places and other files that he knew nothing about. The Alberta group also highlighted this as a serious issue: correcting a mistake in one place in no way ensures it has been corrected throughout the system. A second participant recounted the experience of a friend, who had been diagnosed with HIV based on a mix up of records. The letter informing him of his diagnosis was sent to his home and

opened by his parents. Although the mistake was rectified, ten years later he still cannot give blood as he is 'red-flagged' by the Canadian Blood Service computer. A third participant had an acquaintance who had fought for years to have a diagnosis on her file changed and only finally succeeded after going to the media.

4.6.3 Redress: What can I do if inaccuracies are found in my personal health information?

Very few participants believed that it would be easy to correct an inaccuracy in medical records, although one suggested that it would probably depend on the nature of the change, with more black and white information much easier to change than doctor's opinions. Some thought it might require appearing before some sort of medical review board. Others who had experienced this problem concurred that it was not easy at all, although one Albertan participant noted that he had been able to change a mistake in his file only because of his longstanding, good relationship with his doctor. A few participants in the Francophone group suggested that doctor's opinions should not be subject to revision, since they were just that, opinions. Among survey respondents, most said they would attempt to correct any inaccuracies by going to their doctor or the hospital, depending on who was responsible for their file.

4.7 Data Retention and Protection

4.7.1 Data retention

Consumers were not asked directly to comment on the issue of data retention and it was not raised spontaneously as an issue of great concern other than in the context of consent as an ongoing process. Some focus group participants were strongly against a one-time signing off of the right to control how personal health information would be used, suggesting that consent must be ongoing and revised to reflect new information on file and new potential uses of that information. One participant suggested that if someone wants the right to use the information for a specific purpose, they should be willing to take the time to explain the purpose. Another participant suggested, however, that data on file are a valuable resource and should be available for research if the research benefits society. Again, here we see the tension between personal control and societal benefit.

4.7.2 Data protection

There was considerably greater concern expressed over the need to ensure personal health information is protected. While a small number of participants believed that personal health information was well protected by law, many more thought that access occurs much more frequently than we realize and that personal health information is not well protected at all. Especially in the context of the electronic age, the view was expressed that information is

copied and recopied, transferred from here to there and that while there is probably no widespread intent to compromise privacy, the fact is that many people actually get information they should not have. Many examples were adduced, from individuals talking in hospital corridors, to office staff making test appointments where they could be overheard, from personal health information on discarded hard drives to customs officials reading the specifics on prescription bottles, from wrongly addressed mail to messages left on shared answering machines. Overall the consensus of the Alberta group perhaps best captures the views of the focus group participants across Canada: the current protection of personal health information is viewed as inadequate and haphazard.

When asked directly how concerned they were about the security of electronically stored personal health information or paper records of personal health information, survey respondents expressed a fairly high level of concern over both (a mean rating out of 5 of 3.5 (SD 1.3) and 3.2 (SD 1.3), respectively), suggesting that one is not viewed as much 'safer' than the other. Respondents also indicated a high level of concern regarding the accidental disclosure of information (mean rating 3.4, SD 1.3) but an even higher concern that some personal health information was being disclosed on purpose (mean rating 3.7, SD 1.4).

Of the 76 survey respondents who chose to answer a question regarding whether they had ever experienced a breach of confidentiality, 15 per cent indicated they had, although many declined to share the nature of the breach. Most cases noted in survey responses involved discussion of symptoms or case details in an inappropriate setting, that is, somewhere that was not very private. More serious lapses were mentioned by some focus group participants. For instance, one participant was given information regarding another patient's condition (breast cancer) because they had the same name. In another case, an expectant mother was challenged about her benefits because she was using a midwife and not a physician. The employer challenging her right to benefits should not have been privy to that information. One participant, without sharing any details, indicated that unauthorized release of medical information from her file almost caused her to lose her daughter and that she did not make any attempt to follow up why or how the breach had occurred for fear of drawing attention that may again put her situation with her daughter in jeopardy. In the focus group discussions, it was also clear that many participants were aware of others who had experienced breaches of confidentiality, even if participants themselves had not.

When asked what they would do should they ever experience a breach in confidentiality, most individuals suggested they would start with their doctor and try and identify where the breach had occurred. Many recognized that it might be very hard to clearly identify who was responsible, so any assigning of blame would be difficult. Among other entities that might be approached were regulatory bodies, hospital administrations or ombudspersons, or in some cases a lawyer. In general there was a lack of certainty regarding what process to follow, with many respondents indicating they had no idea. Among focus group participants, many individuals had never heard of the Federal Office of the Privacy

Commissioner. Only one survey respondent (from the mail-in/email sample) suggested that office as a potential recourse.

There was also recognition that many potential courses of action were unlikely given the high cost involved, both in terms of money and time. Furthermore, the irony was not lost on many participants that a breach of confidentiality about medical information implied a desire to keep information private, while any steps taken to seek redress are likely to involve greater and greater promulgation of the information, thereby worsening the situation, not bettering it.

4.8 Lessons learned

Most focus group participants believed that they would approach this issue differently in the future having taken a small amount of time to consider the complexity of the issues. Some will read their consent forms more carefully, others may actually modify them now that they know that this is an option. There was widespread agreement on the need for more public education so that others too could be aware of what was at stake in this debate. Some felt that individuals need to take greater responsibility for their own information and not just assume it is protected. Some more pessimistic participants felt it was a losing battle. Others, in the words of a Manitoba participant, felt that "[we] can put up walls... they are going to keep getting breached, but we've got to keep putting them up, so we don't live in chaos".

4.9 Summarizing the consumer view of privacy and the protection of personal health information

It is encouraging that a small sample of Canadians, without any formal background on the issues and with at most two hours of reflection, were able to make a useful and thoughtful contribution to this debate. The feasibility of seeking and getting meaningful consumer input to policy issues that are central to Canadian life, even if those issues appear complex, was thus reaffirmed. Although a single unanimous position did not emerge, some areas of agreement were nonetheless clear:

- Privacy is an important issue and Canadian consumers should be made more aware of the current situation and the implications of greater or lesser privacy. Public education should be a priority.
- Informed consent should be simplified and clarified and those who wish access to personal health information, especially for secondary purposes should be willing to take the time to explain why.
- Consent for treatment should not be assumed to imply consent to share personal health information other than for the continuing treatment of a patient's illness, for example by sharing information with a specialist.

- Patients should be able to access their own personal health information and should not be charged more than the price of a few photocopies, if they wish a copy.
- Whenever possible, de-identified personal health information should be used wherever possible for secondary purposes and a reasonable attempt should be made to ensure it cannot be re-identified.
- Research is important to Canadian consumers and every effort should be made to avoid impeding research that will benefit society. However, many consumers want to know more about the specific research projects that require their personal health information and some wish the right to refuse consent if they object ethically to the research or find it non-compelling.
- Entities that wish to use personal health information for commercial profit should not be given access to personal health information without explicit consent. Many felt this even extended to de-identified personal health information.
- Redress procedures for cases where confidentiality is breached must be made clearer to the public. People simply don't know where to go or what to do.

The principal area of disagreement was the overall level of personal control that Canadian consumers should have over their personal health information. As noted above, several individuals argued adamantly for total personal control of personal health information, while others believed the system simply had to become more consistent and transparent and they would like to see wide sharing of personal health information without close personal control. The balance shifted in the survey, though, where individuals were asked who should require explicit consent to access their personal health information. Respondents felt that explicit consent should be required more frequently than is currently the case. Similarly many consumers believed consent must be ongoing, so that as the nature of the personal health information changes (for example new additions to a medical file) or as the intended use of the personal health information changes, consumers want to have a chance to revise their consent. Various potential compromises and solutions were put forward in the course of the focus group discussions, but none could be said to have garnered consensus.

5 Analysis of Canadian Legislation

5.1 Introduction

This section of the report compares the Alberta, Manitoba, and Saskatchewan Acts concerning Health Information Privacy, as well as the Draft Ontario Privacy legislation and the Protection of Personal Information and Electronic Documents Act, hereafter referred to as the *PIPEDA*.75 For clarity's sake, this report will refer to the various Acts as the Alberta Act (etc) rather than their (very similar) actual titles. The Statutes are compared on how they deal with a number of issues, which are detailed below in section 5.2. Discussion about how each issue is dealt with in the Acts follows, in section 5.4.

Legislation covered in the analysis

Jurisdiction	Acts	important dates
Alberta	*Health Information Act*	Passed 1999
Manitoba	*Personal Health Information Act*	Passed 1997
Ontario	*Privacy of Personal Information Act*	**DRAFT** - 2002
Saskatchewan	*Health Information Protection Act*	Passed 1999 - **Not yet proclaimed**[76]
Canada	*The Protection of Personal Information and Electronic Documents Act*	In force: (generally) January 1, 2001 (for health information) January 1, 2002

Section 2.4 in the methodology section, above, explains why the particular Acts were chosen. The two most important reasons are essentially because these Acts, and the proposed Ontario Act represent the latest legislative entries in the field and, in the case of the provincial Acts, are the ones which were developed specifically to deal with the entire health care field in their respective jurisdictions.

Some of the other legislative responses relevant to health information privacy in Canada are discussed in section 5.4. It is important to note that these statutes do not constitute the entire legal environment. There are codes of practice, professional ethics, rules and laws which apply to the health care sector, insurers and government, which influence how these players deal with information. As well, of course, there are other statutes and the common law which affect all of the participants in the health care sector.

[76] "Bill 29, *The Health Information Protection Act*, was tabled in the Saskatchewan Legislative Assembly on April 23, 1999. On May 6, 1999, the Lieutenant-Governor gave Royal Assent to *The Health Information Protection Act*. However, the Act does not come into force until proclamation, which has been delayed to allow time for trustees to prepare for compliance." - **http://www.health.gov.sk.ca/ph_br_health_leg_hipamain.html**

5.2 Introduction to the Issues

For this report several issues were examined in each of the statutes[77]. The issues follow the general order of the issues discussed above, in section 1.8, Research themes. The issues were chosen because they had engendered the most discussion in the privacy community and were the ones most likely to be of concern to consumers. Given the limited resources available, it was only possible to give cursory attention to some issues, such as the role of the Commissioner or other oversight body. In this particular case, comparisons were made only with regard to what body is charged with redress and where a consumer would go for help. In other cases, such as the issue of consent, the Acts were more thoroughly investigated not only in an attempt to determine what nuances in the different approaches might be revealed, but also to grapple with the complexities of the Acts and their application to the real world.

5.2.1 Consent

The Acts allow consent to be implied, perhaps to be certain to cover all emergency situations. As well, for administrative ease, a statute can allow for implied consent where express consent has already been given, either for similar purposes, or similar bodies, for the purpose or to the organization stipulated as permissible in the consent. This avoids the ridiculous scene of a patient having to sign consents to collect information at every doctor's visit, or to release information to every specialist consulted on a difficult case.

Whatever form it takes, consent is central to a patient's control of information about him or herself. This report compares how consent is generally understood in the statute, and whether the statute requires that any consent be informed. When a patient does consent to information being collected, used or disclosed, the issue arises as to whether there are any limits to the consent, either that are automatically applied by statute or that can be stipulated by the patient. Those limits relate to the scope of the consent, such as the time the consent is in effect. Other examples of limits are allowing disclosure for some purposes but not others, or allowing use by certain bodies but not others. The report compares whether there are any provisions in the Act that prohibit requiring a patient to give consent for the collection, use or disclosure of information about him or herself, in order to receive particular services.

5.2.2 Other issues

Of course this report is not a comprehensive review of all the issues relating to personal health information privacy. One area that was not addressed in this section involves the issues of de-identified information, data matching and electronic storage. Although the outcome of de-identifying processes affect the consumer, the Acts reviewed generally deal

only with personally identifiable information, and so that is what is reviewed. There is some discussion of de-identified information to the extent the Acts do relate to it, in the section comparing the definitions of personal health information (section 5.3.2).

The development of electronic record keeping, and the greater ease with which personal health information can be shared is certainly behind the development of personal health information statutory rules. However, these rules are designed to provide guidance to organizations; what consumers need to know is whether they provide sufficient safeguards to protect personal health information, which is what this section attempts to review. The extent that security procedures and processes utilize or should utilize de-identifying methods is beyond the scope of this section, and warrants further study.

5.3 Comparative overview of the Statutes

5.3.1 General Approach of the Statutes

The Acts vary in approach. The *PIPEDA* is the most general, covering, as it does, personal information collected, used or disclosed in the course of commercial activity.[78] Much of the concern over how the *PIPEDA* will impact the health community revolves around its being limited to commercial activity, as that line can be difficult to draw in the health care sector, particularly with regards to research.

The provincial Acts cover the entire health sector, without differentiating between commercial and other activity. Ontario's draft Act also covers non-health related personal information, but it has the most specific requirements for health care information of all the Acts. It is also one of the most difficult Acts in which to identify all the rules which affect personal health information because it includes rules for health information held by organizations that are not "health information custodians" separate from the rules for organizations which are.[79] In between the two extremes (the *PIPEDA*'s generality and the specificity of the draft Ontario Act), the statutes of Saskatchewan, Alberta and Manitoba seem easier to follow. This is in no small part because they are setting out the rules for health care only, and not general-purpose privacy provisions. Even among these three, there are quite different approaches.

The Saskatchewan and Manitoba Acts are commendably easy to read, providing an average person an opportunity to understand the rules which affect personal health

[78] The *PIPEDA* does not apply to all organizations, but only those, which fall under federal jurisdiction, until 2004, when it will apply in all provinces that have not enacted substantially similar legislation.

[79] Perhaps this difficulty is an artifact unique to this examination. In most real applications of the Act, one would presumably know what sort of organization holds the information in question, so the confusion of trying to find the rules for all cases would disappear.

information. However, they are not so detailed as the Alberta Act, and thus may not afford as much guidance to organizations attempting to implement appropriate policies.

All of the Acts surveyed emphasize individuals' access to information about themselves. In other aspects, however, the Acts differ slightly, but importantly, in how they define key terms. Three definitions are fundamental to understanding what is protected by the Acts:

1. how the Acts define what information they will include - or what the Acts apply to - is reviewed in Definitions of personal health information in the Acts, 5.3.2

2. how the Acts classify those persons or organizations who will be subject to special rules when they collect, use or disclose personal health information - who the Acts apply to - is reviewed in Organizations in the Acts, section 5.3.3; and

3. how the Acts set up a separate body to review access to personal health information for research (if they do) - who decides in cases of collection, use and disclosure for research - is discussed in section 5.3.4, Research ethics boards.

The first, for the purposes of generality, is referred to in this report as "Personal Health Information". The second is identified using the most inclusive term, "organizations", although each Act makes further distinctions as to which organizations the Act includes or does not include in its definitions. The third definition relates to what will be referred to in this report as a Research Ethics Board (REB) although again the Acts use a number of different terms, and have a variety of approaches, which are discussed below.

The following discussion highlights these concepts of note regarding the general approach employed by the Acts. The discussion is broken down into four sections: the first two discuss common components in all the Acts; the third, a concept (of REBs) which occurs in nearly all the Acts; and, the fourth, section 5.3.5, will discuss items that only occur in one Act, the Saskatchewan Health Information Network and the health data institutes in the draft Ontario Act.

5.3.2 Personal Health Information in the Acts

The treatment and definition of personal health information varies among the Acts. The definitions are included in appendix A for ease of comparison.

The Alberta Act refers to personal health information as simply "health information", rather than personal health information, perhaps because its definition includes "health services provider information". It is notable that the Alberta Act, like its Manitoba counterpart, only includes records in its definition of Health Information, as opposed to the Acts of Saskatchewan and Ontario and the *PIPEDA*, which include information in any form, presumably including conversations.

Alberta's Act divides health information into three subsets, the most important of which, for the purposes of this report, is "diagnostic treatment and care information". This includes the most sensitive information, much of what other Acts refer to as personal health information, information about "the physical and mental health of an individual". As well, the definition includes a short list of other information, such as information about drugs or donations of body parts, "the amount of any benefit paid or payable…" and concludes with "includes any other information about an individual that is collected when a health service is provided to the individual" as long as it is recorded in some way.[80] It does not specifically include genetic information.[81]

The Alberta Act distinguishes registration information so that it can be separately referred to and regulated. Registration information includes demographic information, with the individual's personal health number, location and contact information, as well as health service eligibility and billing information.

The third part of the Alberta definition is "health service provider information". This part does not fit into the central mandate of this research project, as it covers the information about the provider and not the recipient of health care. However, what an organization may do with information about a health care provider may be of concern to consumers because that information may, by inference or data matching, reveal something about them. It is interesting to note that some of what is defined as "health service provider information" is information the *PIPEDA* designates as personal information, and the rest is more professional information, some of which would be found in directories, and so is exempt from the *PIPEDA*. Presumably the drafters of the Alberta Act have attempted to head off any discussion about what sort of information the government can collect on health care providers, providing it with access under specified conditions to information it may require for analysis or planning ~~of~~ related to the health care system.

As well, the Alberta Act makes a distinction between "individually identifying" and "non-identifying" information. "[I]ndividually identifying", when used to describe health information, means that the identity of the individual who is the subject of the information can be readily ascertained from the information;"[82] whereas, "non-identifying", when used to describe health information, means that the identity of the individual who is the subject of the information cannot be readily ascertained from the information"[83]. This distinction is somewhat different from the approach of other Acts, which state that the entire Act only

[80] See, the Alberta Act s.1(1) definition of diagnostic, treatment and care information

[81] The only mention of genetic information in the AB act is in s.22(2)(e)(I) – That subsection allows the custodian to collect information from an individual other than the subject of the information, (*inter alia*) when "assembling a family or genetic history". Note that this is not the same as information about predictive genetic testing, specifically protected in some other Acts.

[82] Alberta, definitions,s.1(1)(p)

[83] Alberta, definitions,s.1(1)(r)

covers information which is identifiable, although the definition of what constitutes identifiable differs. That definition is included in the discussion about each Act that follows.

The Manitoba Act is an example of how an Act can state that it will only affect information that is personally identifiable:

> **"**This Act does not apply to anonymous or statistical health information that does not, either by itself or when combined with other information available to the holder, permit individuals to be identified."

In the Manitoba Act, personal health information is broadly defined, although it includes only recorded information. "[T]he individual's health, or health care history, including genetic information about the individual," is covered, as well as a few other specific inclusions. In the Ontario draft Act, both personal information and personal health information are defined, the latter a subset of the former. The definition of "personal information" repeats the subsection (a) of the definition of personal health information, which deals with the issue of what determines that information is personally identifiable. The Ontario draft Act continues:

> "…and includes personal health information and information that relates or may relate to the work performance of the individual or professional wrongdoing, misconduct or disciplinary matters involving the individual, but does not include organizational information or professional identity information"[84].

This elaboration is presumably to prevent the kind of disagreement that has arisen over interpretations of personal information in the *PIPEDA*. There has been some controversy in the interpretation of whether the collection of physicians' prescribing patterns by international companies constitutes a contravention of the *PIPEDA*. The Privacy Commissioner, responding to a complaint by a physician, found that the prescriptions were a "work product" and not personal information of the physician.[85] Under the Ontario draft Act, this "work product" is specifically included in the protections for personal health information.

The Saskatchewan Act's definition of personal health information is nearly identical to that in the *PIPEDA*[86], except that Saskatchewan adds the subset of "registration information". These definitions are the broadest of the Acts reviewed:

[84] Ontario draft Act, s.2, definitions, "personal information"
[85] See discussion of the Privacy Commissioner's findings on his website, and the actual wording of the letter of findings, October 2nd, 2001. Discussion: **http://www.privcom.gc.ca/cf-dc/cf-dc_010921_e.asp** Findings: **http://www.privcom.gc.ca/media/an/wn_011002_e.asp**. These findings are being appealed. See The Privacy Commissioner of Canada, *Annual Report to Parliament 2000-2001*, p.105.
[86] *PIPEDA* s.2(1)

> **"personal health information"** means, with respect to an individual, whether living or deceased:
>
> (i) information with respect to the physical or mental health of the individual;
>
> (ii) information with respect to any health service provided to the individual;
>
> (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (iv) information that is collected: in the course of providing health services to the individual; or,
>
> (B) incidentally to the provision of health services to the individual; or,
>
> (v) registration information[87]

Registration information is defined in the Saskatchewan Act in a manner similar to the way in which it is defined in the Alberta Act, but in less detail. Note that the Saskatchewan Act expressly limits its application, by stating it does not apply to:

> (a) statistical information or de-identified personal health information that cannot reasonably be expected, either by itself or when combined with other information available to the person who receives it, to enable the subject individuals to be identified;
>
> (b) personal health information about an individual who has been dead for more than 30 years; or
>
> (c) records that are more than 120 years old.[88]

The *PIPEDA* likewise does not apply to information that does not pertain to an identifiable individual. Its definition of personal information is very broad:

> "personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."[89]

Neither the Saskatchewan Act nor the *PIPEDA* mention genetic information specifically.

[87] SK s.2(m)
[88] SK s.3(1)
[89] *PIPEDA* s.2(1)

Table 5.3.2. is provided as a summary of discussion in this section.

Table 5.3.2

Personal Health Information (PHI) in the Acts – an overview				
Province/Act	**Records** only?	**Identifiable** only? (if yes, whole Act or by definition?)	**Termination** of designation as PHI	**Genetic Information**? Other subsets?
Alberta	Yes	No – defines identifiable and non-identifiable	None	3 parts to "health information"
Manitoba	Yes	Yes - Whole Act – s.3	None	Genetic info included in PHI definition
Ontario draft	No	By definition, PHI	None	Genetic info separately defined
Saskatchewan	No	Act, s.3(2), does not apply to de-identified information	Records greater than 120 years	No
PIPEDA	No	Yes - by definition: personal information, personal health information[90], and by Act's application –s.4(1)	Disclosure allowed after the earlier of 100 years after record was created and 20 years after death of subject individual.[91]	No

5.3.3 Custodians, Trustees or Organizations entrusted with personal health information

The list of those bodies permitted to collect, use and disclose information under the Acts can be long. Different terminology is used:

- "**Trustee**" – Saskatchewan, Manitoba,
- "**Custodian**" – Ontario's draft, Alberta,
- "**Organization**" – *PIPEDA* (and Ontario's draft when it means a body other than a health information custodian)

In Ontario, any organization can hold personal health information, but there are specific rules for the subset of organizations that are health information custodians. Generally, these rules give a wider latitude to health information custodians dealing with PHI, when dealing with one another. This wider latitude is designed to assist the efficient functioning of the health care system by sharing health care information.

These definitions of trustee, custodian and organization determine the applicability of an Act to an organization. The approaches vary from including the widest possible range, as

[90] *PIPEDA* s.2(1)
[91] *PIPEDA* s.7(3)

in the *PIPEDA*, to specific listings of groups. The *PIPEDA* states simply that an ""organization" includes an association, a partnership, a person and a trade union."[92] The Alberta Act's definition is detailed and very long. In between is the Manitoba Act's approach, which lists the general groupings or subsets of "trustee", and then defines them separately.

Comparing the lists of what are considered trustees or custodians, the definitions generally reflect many of the same organizations. However, there are some differences among the Acts, in particular what specific public or quasi- public bodies are included.

The sometimes-long definitions are reproduced in Appendix B to allow a comparison of where in the different Acts the line is drawn between public and private organizations, and how the organizations included are grouped.

The definitions of custodian, trustee or organization in all the Acts reviewed in this study include the provinces' respective ministries of health and other public bodies. (Naturally, the *PIPEDA*, as a federal law, dealing with the private sector, does not.) Although each province includes its Ministry of Health, as a trustee or custodian, each provincial Act may or may not allow for separate rules for public bodies to access, use or disclose personal health information for the purposes of analyzing or administering the health care system. These differences are discussed below, under research, in section 5.4.6.

5.3.4 Research Ethics Boards

The third issue fundamental to the understanding of the Acts is the different approaches used to determine who should get access to personal health information for research purposes. One approach to the problem is to have such research approved by an ethics board or a similar organization. Each provincial Act employs some variation on this theme. For consistency, where speaking of the review panels generally, this report will refer to them as Research Ethics Boards, or REBs. The different Acts have different requirements regarding the REBs' constitution, governance and accountability, as follows.

The *PIPEDA* does not provide for a separate body to review research, but the Privacy Commissioner must be informed before information is used without consent for the purposes of research.[93]

[92] *PIPEDA* definitions, s.2(1)
[93] *PIPEDA* s.7(2)(c), (use), and 7(3)(f) (disclosure)

Table 5.3.4

Province/Act	Names of REB	Established by	Reporting or other requirements
Alberta	Ethics committee	Designated by regulation	See Alberta Act, s.50
Manitoba	health information privacy committee/	Minister	See Manitoba Act s.59
	institutional research review committee	health care facility, university or similar body	See Manitoba Act s.24
Ontario draft	research ethics board	In accordance with regulations	Annual report, written policies, written decisions with reasons
Saskatchewan	research ethics board	Approved by minister	none
PIPEDA	none	none	Privacy Commissioner must be informed[94]

For more details on each Act's approach to research, refer to section 5.4.5 in the discussion below.

5.3.5 Other distinguishing features of the Acts

Besides the development of the research ethics board concept, two provinces also introduced in their legislation new procedures and protections for information. Saskatchewan's Saskatchewan Health Information Network and the health data institutes included in Ontario's draft Act are discussed below.

5.3.5.1 Saskatchewan Health Information Network

Saskatchewan's Act includes the Saskatchewan Health Information Network" (SHIN), which is a "Crown corporation established pursuant to The Crown Corporations Act, 1993 to create and maintain a networked electronic health record for the purpose of sharing personal health information between trustees throughout Saskatchewan".[95] SHIN, though set up to share information for the benefit of the health care system, affords some controls to affected individuals. In s. 8 of the Saskatchewan Act, a trustee must take reasonable steps to inform individuals that he or she has entered into an agreement to use SHIN. Also in s. 8, an individual may require that a trustee not include information pertaining to that individual on SHIN, or prevent that information being accessed by other trustees if it is included.[96]

[94] *PIPEDA* s.7(2)(c), (use), and 7(3)(f) (disclosure)
[95] SK s.2(r)
[96] SK s.8

5.3.5.2 Ontario's draft Act – health data institutes

Ontario's Draft Act introduces the "health data institute" in s. 47, which must be approved by the Minister, and reviewed annually by the Commissioner, as required in s.47(13) if :

> …(c) its corporate objects include performing data analysis of personal health information, linking the information with other information and de-identifying the information for the Minister; and,
>
> (d) it meets all other prescribed requirements.

Duties of a health data institute are then described (s.47, continued).

> (16) A health data institute that receives personal health information under subsection(1) shall, (…)
>
> (e) provide the results of the analysis and linking using only the de-identified information mentioned in clause (c) to the Minister or to the persons that the Minister approves;…

Essentially, the health data institute receives personal health information from health information custodians for the purpose of de-identifying it, for use by persons approved by the minister, who are engaged in the analysis of the health care system. The information disclosed by organizations to the health data institute must be requested by the Minister, after the request is review by a technical committee.[97] If, for some reason, the Minister desires that information without it being de-identified, the Commissioner must review the proposed disclosure.[98]

5.4 Comparative Analysis of the Statutes

This section investigates the same issues raised in the context of the stakeholder groups. The first issues relate to consent regarding personal health information as a whole in the Acts. Then the discussion considers what requirements each Act makes for consent to collect, use or disclose personal health information. The special case of research purposes is subsequently addressed. The discussion then focuses on security safeguards and rules for an individual's own access to information about him or herself, how that information can be corrected, and how to launch appeals when access or correction is refused. The role of the body in place to receive complaints is then briefly touched upon, along with any penalties or statutory rights to compensation.

[97] ON s.47

[98] On. S.48 Note that subsection 48(1) of the draft Act is somewhat unclear as to whether the Minister is obliged each time to seek the Commissioner's approval. The authors assume this will be improved in subsequent revisions of the Draft Act.

5.4.1 Consent

Informed consent is central to privacy as it denotes control over the use of personal health information and the people who use it. The Acts generally make obtaining consent the default position,[99] but that has little bearing on how privacy-friendly the Act actually is, as the sum of all the exceptions and permissions may mean there are few circumstances, purposes or organizations left for which consent is required. Consent is also governed by the Common Law, so that although an Act gives particular rights, these may not be the entire story.[100]

The Acts do not address the ideal world where consent entails completely informed choice. In two Acts, from Saskatchewan and Alberta, the collection of personal health information does not require consent. In those Acts, consent for collection is assumed when patients are informed of the uses to which their information will be put, although most uses or disclosures require consent. This assumption relies on the idea that the information is being collected from the affected person, therefore that person must have given consent implicitly. The other Acts allow consent to be implied in such circumstances, but only where it is reasonable to do so. There are always provisions for necessary, real world exceptions to consent, for reasons of emergency, law enforcement, court orders, etc, and in general, the Acts only differ in their manner of dealing with these exceptions.

5.4.1.1 Informed consent

All of the Acts require consent with regard to personal health information to be informed in some circumstances. Two of the Acts, the Manitoba and Alberta Acts[101], require an individual to be informed, but do not require that he or she consent to the collection of personal health information. The individual must be informed of the uses to which the information will be put: consent for collection is assumed. "Informed" means somewhat different things in each Act. In the Alberta Act, consent to disclose must be in writing (or captured in electronic form) and include:

> "an acknowledgement that the individual providing the consent has been made aware of the reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent." [102]

Ontario's draft Act has similar provisions underlining the need for the patient to understand the implications of his or her consent. Manitoba's Act is not as adamant about demonstrating that an individual has been informed of his or her choices. For example, where the Manitoba Act requires consent, for either use or disclosure of personal health

[99] Except the Alberta and Manitoba Acts – see below section 5.4.1.1
[100] see, for example, the discussion of Torts and Contract law remedies in Ian Lawson, *Privacy and Free Enterprise*, second edition, the Public Interest Advocacy Centre, 1997, chapter 6.
[101] AB s.22(3); MB s.15(1)
[102] AB Act s. 34(2)(d)

information, it requires no demonstration that consent is informed. Where it does refer to "informed consent", in collection, it is only necessary to inform the individual about the purposes for collection, and whom to contact with any questions.

Another approach to the requirement for an individual to be informed is a reasonableness test. The *PIPEDA* requires that:

> "Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed." [103]

Likewise, Saskatchewan's Act requires the personal health information trustee to take reasonable steps to inform the individual.[104]

5.4.1.2 Tied consent and information about consequences

Some of the Acts specifically require the patient to be informed of the consequences of withholding consent and any benefits of giving consent before consent is obtained. Saskatchewan's Act does not require this and neither does Manitoba's. The Alberta Act only requires the information on risks and benefits of consent when the consent relates to disclosure, as set out above. The draft Ontario Act requires "a general understanding of the nature and consequences of giving or withholding consent".[105]

The *PIPEDA* requires an organization to make reasonable efforts to ensure a patient is advised, as above, when being asked to give consent. Only where the purposes are not "explicitly specified and legitimate" does it prevent consent being tied to the delivery of services, because it also states that:

> "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes."[106]

Other statutes provide protection from coercing consent to the collection, use, or disclosure of information by prohibiting the refusal of services without consent relating to personal health information, at least in specific cases. For instance, Saskatchewan's Act (in certain cases) prohibits anyone from being refused services for not revealing his or her

[103] *PIPEDA*, 4.3.2, Sch.1
[104] SK Act, s. 9
[105] ON Act, s.8(4)
[106] *PIPEDA* s.4.3.3 Sch.1

health care number[107]. As well, the Act states that coercion, in general, is not permitted for any collection:

> 6(1) Where consent is required by this Act for the collection, use or disclosure of personal health information, the consent:… (c) must be given voluntarily; and (d) must not be obtained through misrepresentation, fraud or coercion.

Ontario's draft Act prohibits tying service to collection, particularly regarding genetic information, and in general:

> an Organization shall not, as a condition of dealing with an individual, require the individual to consent to the collection, use or disclosure of, (a) personal information about the individual beyond that required to fulfill the purpose of the dealing; or (b) the individual's genetic information.[108]

Manitoba's Act does not deal with the issue of tied consent.

5.4.1.3 Withdrawing consent

There can be far–reaching effects of withdrawing consent to use, disclose or collect personal health information. The *PIPEDA* states that where an individual withdraws consent, "the organization shall inform the individual of the implications of such withdrawal".[109] This provision in *PIPEDA*, applying to all personal information, demonstrates that any services could be affected by withdrawal of consent to information. However, the withdrawal of consent to access information can have more acute effects on the provision of health care. Other Acts also make specific provisions that require the organization ~~to~~ explain the consequences when a patient withdraws consent to collect, use or disclose information. The Ontario draft Act requires the organization to "provide information to the individual of the consequences of withdrawing consent to the collection, use or disclosure of the personal information."[110] The Saskatchewan Act explicitly provides the right to revoke consent.[111] The trustee is not obliged by the Act to detail the consequences of such a revocation, however. Neither the Alberta nor the Manitoba Act make any specific provision for withdrawing consent.

5.4.1.4 Limits to consent

As well as allowing individuals to withdraw consent, a truly privacy-friendly Act would provide individuals the opportunity to add limitations to the scope of consent. Some of these rights are provided by the Common Law, as an aspect of contract law, which

[107] SK, s.11(1)
[108] ON, s.19
[109] PIPEDA s.4.3.3 Sch.1
[110] ON Act, s.12(2)
[111] SK s. 7

establishes the general rule, for instance, that an individual can stipulate the terms he or she will abide by, providing of course, that the other party agrees. It can be assumed, however, that the power difference is such in health care situations that most people do not realize they could alter a consent form placed before them, much less demand certain limitations on what happens to information about them.

Some privacy advocates (and consumers, see section 5) would have consent limited in scope, in a "layered" fashion, so that consent given for collection, for instance does not provide an organization the right to use the information in any way. Layered consent would also allow for consent to disclosure separate from use, or consent to most organizations except specific ones.[112] None of the Acts specifically require the organization to allow consent to be so modified by the patient, but nothing prevents such modifications either. The rules in many Acts, as discussed further below, do differentiate among consent rules for collection, use and disclosure. This affords some extra protections to individuals, although the rules are imposed upon them by the intricacies of the statute, which may not line up with the desires of any one individual. Limits to the scope of consent are provided for in the *PIPEDA*, which allows individuals to refuse to consent to information collection, use or disclosure "…beyond that required to fulfill the explicitly specified and legitimate purposes".[113]

One type of limit to the scope of consent that is more easily grasped, and possibly administered, is the imposition of a time limit on the consent. The Saskatchewan Act requires trustees to allow individuals to place limitations on the duration of consent: "A consent may be given that is effective for a limited period."[114] The Alberta Act gives something of this ability to individuals by expressly requiring a time limit on the consent and permitting revocation at any time, but only for consent for disclosure, and not for collection or use. Manitoba and Ontario do not expressly permit limitations to the duration of consent.

5.4.2 Collection

For each aspect of personal health information - collection, use and disclosure - the question is whether the rules differ depending on who is collecting, using, or disclosing the personal health information, and whether the rules also vary depending on the purposes for which a person or organization is collecting, using and disclosing the personal health information.

As has already been discussed, the Acts of Manitoba and Alberta do not actually require consent for collection. [115] However, there is a specific requirement in the Alberta Act, that

[112] See BCFIPA (need full cite)
[113] PIPEDA 4.3.3
[114] SK Act, s.6(3)
[115] MB s.15(1); AB s.22(3)

if personal health information is collected by video tape or other means that may not be evident to the individual, express written consent must be obtained from the individual.[116] In the other Acts, explicit consent to collect information is required in some cases. The *PIPEDA* generally requires consent to be explicit where consent cannot be reasonably implied.[117] The draft Ontario Act requires explicit consent to collect genetic information by any organization and to collect personal health information by an organization that is not a health information custodian. Saskatchewan allows implied consent for primary purposes, i.e., that which "can reasonably be expected to benefit the subject individual"[118]. It appears that in that Act, consent for secondary purposes "must be express unless it is reasonable for the trustee to infer that the subject individual would consent to the disclosure, and where the disclosure is being made: … [list of approved purposes to imply consent] ".[119]

5.4.3 Use

Approaches to the use of personal health information vary. It is always possible to forgo requirements for consent for use in cases of danger to the public or the subject individual of the information, or other emergency; to alert next of kin or caregivers; or as required by law or court proceedings. The specific provisions may draw these distinctions differently, but since the Acts vary principally according to the methods used to describe the practices already in place for hospitals and other health care providers, they are more or less uncontroversial. Other purposes and organizations using the information are of greater concern, as is the nature of the circumstances that allow for consent to use personal health information to be implied or to require express consent

5.4.4 Disclosure

In all the Acts, disclosure of personal health information for the purposes of direct care to the patient (whether to other health care providers, relatives or caregivers) is either allowed without consent, or consent to disclose may be implicit. As well, disclosure for societal reasons, such as for law enforcement, or for purposes of payment, is allowed either with implicit consent or without consent. Again, the parameters of disclosure to the government for health system purposes and to researchers for academic or product development are often more problematic. Another variation among the Acts is that some require organizations to keep a record of all the disclosures made, while others only require records to be kept of disclosures made without consent, or make no requirement at all.

[116] AB s.23
[117] PIPEDA Schedule 1, s. 4.3.5
[118] SK s.1(2)(o)
[119] SK s.27(3), incorporated into s.24

Alberta requires that an express written consent be obtained in order to make disclosure by electronic means.[120]

The *PIPEDA* allows consent to be implied for disclosure unless it is not reasonable to do so, and only where the use in question would be reasonably expected and approved of in the circumstances.[121] The Act, in Schedule 1, gives the example of a health care professional disclosing information to a company selling health care products as an illustration of a case when consent would not be reasonable to imply.[122] There are specific purposes for which consent to disclose is not required, relating to emergency or national security for example.[123] In the case of research where consent is impracticable, the Commissioner must be notified before the use or disclosure.[124] Also, one hundred years after the record was created, or 20 years after the patient's death, whichever is sooner, the information may be disclosed without consent.[125] The rules for disclosure do not depend on who is disclosing the information. The listed exceptions for various purposes allow disclosure (with no consent) to those persons or bodies that fulfill those purposes[126].

5.4.5 Research-specific rules

As discussed above (section 5.3.4) each of the provinces have provided some form of supervision by a Research Ethics Board (REB) to control personal health information used by or disclosed to researchers. The REBs are usually charged with deciding whether research requires personally identifiable information, and if it is of sufficient importance to warrant the disclosure of that information without consent, where consent is impracticable. In some provinces, more of these tasks are taken on by the organization holding the information, and in others the Commissioner or other body is involved in the oversight of the REB. Notable differences among the Acts reviewed are discussed below.

The Alberta Act details what the ethics committee must consider, including whether the proposed research is of sufficient importance that it "…outweighs to a substantial degree the public interest"[127]. All research involving individually identifying health information is reviewed by an ethics committee, regardless of who held the personal health information proposed to be used in the research.

In the Manitoba Act, the purpose of the research may be considered by the institutional research review committee in determining if the "research is of sufficient importance to outweigh the intrusion into privacy that would result from the disclosure of [personal health

[120] AB s.59
[121] *PIPEDA* Sch.1, 4.3.4 to 4.3.6
[122] *PIPEDA* Sch.1, 4.3.5
[123] *PIPEDA* s.7
[124] *PIPEDA* s. 7
[125] *PIPEDA* s.7(3)(h)
[126] *PIPEDA* s. 7
[127] AB s.50(1)(a)(I)

information]".[128] Other research is also permitted under the Act: research and planning that relates to the provision or payment of health care by a trustee (which would include the province's analysis of the health care system); review by a standards committee studying health care practice; and research and planning relating to health care using a government- (or agent-) established database. Research using personal health information held by government custodians is to be reviewed by a different body, a health information privacy committee, as compared to the institutional research review committee for privately held information. The fact that these two bodies could be quite differently constituted may lead to different rules in practice, although the conditions for approval for both types of committees are the same.

In the draft Ontario Act, health research with no consent, using personal health information held by a health information custodian, is permitted only as reviewed by a REB. Other organizations wishing to use personal health information for research must obtain the approval of the Commissioner. Because of this difference, different bodies do have different rules in the Act about the need to obtain consent for research purposes. Health data institutes, which provide de-identified information for research into the health care system, follow a separate rule again. The decision to have health information disclosed to health data institutes is reviewed by a technical committee and the Commissioner, with final approval by the Minister. Decisions to have the health data institutes disclose personally identifiable information to the Minister are reviewed by the Commissioner.

Research is defined in the draft Ontario Act as follows:

> "[R]esearch" means a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research;"[129]

Research using personal health information without consent is permitted only as reviewed by a REB in that Act. The research ethics board considers the ethical balancing question as well as whether the research could be performed with de-identified information, and ensures that proper safeguards are put in place. However, the trustee must also be of the opinion that "the research project is not contrary to the public interest"[130]. The rules do not vary for research, neither depending on either the body performing the research nor the trustee maintaining the information required.

Another form of research considered by Ontario is quality assurance. That province has proposed a new Act, to supplement its draft privacy Act, which will allow organizations to convert personal health information into quality of care information, which cannot be

[128] MB s.24(3)(a)
[129] ON s.2
[130] SK s.29(1)(a)

accessed or disclosed for other purposes. This development is intended to promote free discussion within the organization, to improve patient care.

The *PIPEDA* requires that disclosures for research where consent is impracticable must be reported to the Commissioner before disclosure. However, individual consent to use personal information is required if the research purposes can be achieved with anonymous information. [131]

5.4.6 Protection of Data

All of the Acts require that the custodians, trustees or organizations of personal health information keep it safe. The Acts which cover both personal information in general as well as personal health information include requirements for extra protections for sensitive information.

The *PIPEDA*, for instance, requires that "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information."[132] Ontario's draft Act has a nearly identical statement in its purposes section[133]. As well, it requires that decisions about protection "be determined in light of all the circumstances, including the sensitivity of the information…"[134] Manitoba's Act also requires that the sensitivity of the information be considered in determining the reasonableness of security safeguards.[135] Alberta and Saskatchewan make no mention of differentiating the level of protection to relate to the level of sensitivity of the personal health information. Presumably they assume all personal health information is sensitive.

5.4.6.1 Duration of storage

The *PIPEDA* requires that information not be kept longer than necessary for the purpose for which it was collected. The Ontario draft Act uses this same stipulation, with some exceptions, where the organization is otherwise required to retain the information. In Alberta, Saskatchewan and Manitoba, the organization is required to establish policies regarding information storage, and except in the Alberta Act, the Acts stipulate that these policies must cover destruction.

5.4.6.2 Movement to archives

All of the Acts have some stipulation to allow information with historical relevance to be moved to some form of archives. In some cases the archives are themselves included as a

[131] PIPEDA, s.7(2)(c), 7(3)(f)
[132] PIPEDA 4.3.2
[133] ON s.1(b)(iii)
[134] ON s.50(1)
[135] MB s.19

trustee or custodian, facilitating the movement of information to them, and in other cases they are exempted from requirements for consent to disclosure.

5.4.7 Individual's own access, correction of information, and redress

As stated above, each Act provides consumers with an avenue to access their own information. Each Act requires that the process be "open". The Ontario and Saskatchewan Acts take this openness a step further. The Saskatchewan Act requires the trustee to "promote knowledge and awareness of the rights extended to individuals by this Act, including the right to request access to personal health information and to request amendment of that personal health information."[136] Ontario's draft Act requires organizations to make available a statement describing how to access personal information.

All of the provincial Acts require that an individual be able to get a copy of records, and provide that organizations can charge a reasonable fee to make a copy.[137] The *PIPEDA* states that the requested information shall be provided or made available in a form that is generally understandable.[138] Some Acts prescribe that an individual be told what the fee would be (before the individual is provided with the copy). The Ontario and Alberta Acts require the custodian to provide processes regarding waiving that fee under certain circumstances, including if the custodian feels the fees would prove a financial hardship to the requesting individual.

In all the provincial Acts the organization is required to "provide an explanation of any term, code or abbreviation used in the record"[139], to quote the Alberta Act. The Alberta and draft Ontario Act, state that this duty is qualified by "if reasonably practical". In the Saskatchewan Act, if the trustee is unable to provide an explanation, the trustee must refer the applicant to a trustee who is able to provide an explanation. The *PIPEDA* states that "the organization may choose to make sensitive personal information available through a medical practitioner"[140], which may have the effect of allowing for greater explanation, as well as sensitivity, in disclosures.

The Saskatchewan Act requires the trustee to record a list of those parties to whom the trustee has made disclosures, with no consent, of an individual's personal health information, and that list can be requested by the individual. All the other Acts, except Manitoba, require that a list be kept of all disclosures, and shared when access is requested by the subject individual. In Ontario, it seems that access to a health care custodian's record of disclosures must be given when other information access requests

[136] SK s.9(3)
[137] Cites for copying sections in all Acts
[138] *PIPEDA* Sch.1 4.9.1
[139] AB Act, s.10(c)
[140] *PIPEDA* Sch.1 4.9.1

are made[141]. If health care information is maintained by another organization (which isn't a health information custodian) in that province, it must provide access to the disclosure list if the person referred to in the record specifically requests it[142]. Similarly, the *PIPEDA* and the Alberta and Saskatchewan Acts require that an organization allow access to a list of disclosures if specifically requested[143]. The Manitoba Act makes no requirement that a trustee keep a record of who has accessed information about an individual.

5.4.7.1 Access denied

There are circumstances provided in each Act where an organization can deny an individual access to his or her own files. These differ, but all presume that there are circumstances in which it may not be in individuals' best interest to see what is recorded about themselves.[144] Each Act specifies that the organization holding the information decides if it is appropriate to withhold access in these cases, but the Acts provide some kind of review for such decisions.

Generally, if access is denied, the organization must reveal why, at least in general terms, and especially when it was denied for safety reasons. The Alberta Act takes the approach that there are some reasons why a custodian may refuse to allow access, and others where they must refuse, such as when access would reveal the results of a criminal investigation. These same reasons are considered permitted reasons to refuse access in other Acts. The Acts generally provide for an organization to refuse access for other reasons. For example, the Saskatchewan and Manitoba Acts allow trustees to refuse access to information collected solely for peer review or other professional review processes, or where confidentiality of information from another individual would be broken. The Ontario draft Act also allows a custodian to refuse frivolous or vexatious requests.

As well, all the Acts, except Alberta's, state that as much information as possible should be disclosed to the individual concerned, with the offending information severed.[145] Though the duty to sever is not in the Alberta Act, the Act does contemplates release of part of the personal health information in question.[146]

[141] by inference from s.51(1) and s.57(17) of the draft Ontario Act which provide that organizations other than health information custodians must provide such information if access to the list is requested by an individual.
[142] ON s. 57(17)
[143] *PIPEDA* Sch.1 4.9.1; SK s.10
[144] Some privacy advocates believe that the purported need for such provisions has not been adequately proven, and that any ability to restrict access to information about oneself should be far more limited.
[145].SASK s.38(2); MB s.11(2); ON s.57(11), 60(10); PIPEDA s. 9(1)
[146] AB s.12(2)(c)

5.4.7.2 Appeal

If an individual wishes to appeal a refusal to access information, the organization is required to inform him or her of the appeal process, which is described in each Act. One option in all cases is to place a complaint with the Commissioner (or, in Manitoba, the Ombudsman) if access is refused because of concerns of potential harm to the individual.

5.4.7.3 Correction

All the Acts also provide a process by which individuals, who believe information about themselves to be inaccurate, can request that it be corrected. The process is required to be "open" or transparent in each Act. Again, the Saskatchewan Act imposes a positive duty on the organization to promote awareness of these provisions.

In general, if the organization does not agree with the individual, and refuses to change the record, there are clear provisions, which require that the organization give the individual the option of adding a note to the record to the effect that the individual does not agree, or contesting the organization's decision. There are differences in exactly what process is required. The organization is required to provide information on how to go about contesting a decision, again to the appropriate Commissioner or, in Manitoba, the Ombudsman.

5.4.8 Review (Commissioner)

Each Act provides for a Commissioner (or Ombudsman, in Manitoba) to investigate complaints and generally review adherence to the Act. The workings of these offices vary greatly, but the process for initiating a complaint does not differ greatly between provinces, although some would require a complaint in writing. The Commissioners may instigate investigations on their own, and generally have powers to have non-adherent practices stopped and ill-gotten information destroyed. Their decisions can be enforced by court orders as well.

5.4.9 Penalties

Table 5.4.9
Penalties as provided for in each Act for offenses listed.

Province/ Act	Penalty personal up to $	Penalty - corporate up to	Statutory right to damages
Alberta	$50,000	Same as personal	No
Manitoba	$50,000	Same as personal	No
Ontario	$50,000	$250,000	Yes
Saskatchewan	$50,000	$500,000	No
PIPEDA	Not specified	Not specified	Yes

Damages and publication orders are possible under PIPEDA, but only where the individual or Commissioner has taken the issue to court.

6 Gap analysis and Recommendations

6.1 System knowledge dissemination

Consumers admit that they have little knowledge about and perceive themselves to have little control over what is happening to health information about them. Despite the burgeoning use of electronic records, information may not always be widely shared as yet, but it is important to note that limited information flow does not mean that there is ultimate privacy. Information held in an insecure environment, over which an individual has no choice or control, is not truly private.

Knowledge of the processes and rules used to control information flows is problematic. The processes are theoretically transparent, but are actually obscure to the individual. An "open" process is required by statute in all jurisdictions studied, however, legislation provides few approaches to ensure, in practice, that the access and correction process is transparent and well communicated. One piece of legislation, which seems to foster an open system and promote consumer knowledge, is the Saskatchewan Act. It requires organizations to promulgate individuals' rights under the Act. Stakeholder groups agree on how important open systems are and recommend that consumers should be informed about their rights in the health system regarding consent to information flows and redress. However, consumers' current level of understanding and awareness of information flows in the health system is minimal. This is true both of current and proposed systems. Consumers fear that their personal health information will be disseminated in a way that it shouldn't be, and, in the absence of transparent systems, show a tendency to want tight personal control.

This fear on the part of consumers indicates that there are many unknowns. More information is needed to provide consumers with an understanding of what their rights are and how to ensure they are respected. The understanding consumers have of their rights is contrasted with other stakeholders' recommendations and the legal context in greater depth below. The discussion will review the meaning of, need for, and scope of consent; data retention and protection; access and correction of an individual's own information; as well as consumer rights to redress.

6.2 Meaning of consent

Consumers, other stakeholders and legislators agree that explicit consent must be informed. Being informed means many things. The highest standard for an informed consumer involves the consumer understanding the risks and consequences of consenting to the collection, use and disclosure of personal health information, or of withholding consent. Several Acts do not insist that this standard applies. There is acknowledgment in some but not all of the statutes that consumers need to be made aware of the risks and

consequences of giving consent to collect, use and disclose personal health information. From the research, consumers clearly do not normally consider the risks and consequences of giving consent to collect, use, disclose, and access personal health information about themselves, until faced with a problem. They put a large amount of trust in their health care providers. As well, it seems that consumers may not always be well informed about how their personal information will be used when giving consent and, especially, that the consenting to treatment may mean their personal health information is used for other purposes

From the research, consumers agree that to be informed involves the need to understand or be clear about the uses to which one's personal health information will be put. To consumers, one either gives consent or does not give consent; the concept of "implicit consent" is academic. That said, consumers appear to be aware that in some cases no consent/implicit consent makes sense. They simply want those cases to be clearly defined.

There is disagreement, therefore, among consumers, other stakeholders and legislators, as to what informed consent means and how it should be demonstrated. Statutes also vary in the way that they approach consent, how key terms are defined relating to consent, and particularly which exceptions to consent are allowable.

The concept of implicit and explicit consent is also not consistently applied in the statutes, which increases confusion among consumers and other stakeholders, especially when implied consent is compared to situations where there is no consent required.

> **Recommendation 1**: Educate the public about the risks and consequences of the collection, use and disclosure of personal health information. Identify who is responsible for educating the public and what salient points need to be communicated to consumers in priority order. This public education might take place at the time a consumer is asked to sign consent to collect, use or disclose personal health information for primary purposes. It is important to foster open discussion about these issues without minimizing them by subsuming them in the broader treatment context.
>
> **Recommendation 2**: Reconcile stakeholders' more academic interpretation of consent with consumers' practical interpretation of consent. Use the same language to describe the same concepts so that practical solutions around consent issues can be commonly understood and brought forward for implementation. If the concept of implicit consent is to remain an integral part of this debate, it must be very clearly defined and communicated to Canadian consumers of health care.
>
> **Recommendation 3**: Ensure separation between the consent process for treatment and the consent process for collecting, using or disclosing personal health information for secondary purposes. Consider the possibility of dividing the process for obtaining consent, using the primary/secondary distinction. In other

words, consider obtaining consent to information sharing for treatment at the time of treatment, followed by authorization for other purposes at a different time, when the implications of giving consent for secondary purposes are clear and thus the consumer can be said to be informed. Recognize the need to make forms less onerous and more accessible in general.

6.3 Need for consent

Most consumers and virtually all stakeholder groups agree that consent is needed for the collection use, and disclosure of personal health information (which is generally recognized in the legislation reviewed). Disagreement arises over which circumstances warrant explicit consent, which allow for implied consent, and when (if) exceptions can be made.

Consumers see the act of giving consent to be integral to the process of maintaining control over their personal health information. Nevertheless, most consumers do not read or change the terms of the consent forms they sign. Focus group discussions suggested this stems from a lack of awareness that such changes are possible, that they are important, and/or from consumers' perceptions that consent to treatment is contingent upon consent for information purposes. It also appears to be a function of an implicit trust in the medical system: "if my doctor asks me to do it, it must be OK".

The issue of health privacy is not at the forefront of consumer awareness and there is also no strong political will to address the issue at present. However, although the extensive current debate over the future of socialized health care may contribute to a sense of issue fatigue for taxpayers, it may also represent an opportunity to "tag on" privacy issues, and gain media attention as an alternative angle on the debate.

> **Recommendation 4**: More research is needed to identify which circumstances require explicit versus implicit consent, identifying the specific issues of concern to consumers. There are clear advantages to promoting discussion and debate on this topic. By asking consumers questions about the issue, the issue will come to the fore in individuals' minds, leading them to question and explore how their personal health information is being used. As well, if the population is made aware of the situation, more meaningful responses can be garnered from a more fine-grained research process, involving a larger, more representative, better informed sample.

6.4 Scope, specifically duration, of consent

Information from the three research foci coincide on the issue that there should be clear limits as to how long consent lasts in the collection, use and disclosure of personal health information. There is disagreement, particularly between researchers and other stakeholders, as to what these limits should be. Essentially, researchers would like to have indefinite access to the information used in a given study for other research purposes.–

There is no single common approach to limiting consent in the statutes reviewed. In some statutes, the duration of consent is required to be explicitly stated. In others it can be implied, or the statute requires individuals to be able to put limits on consent. Provisions in the Saskatchewan Act require temporal limits. Most statutes allow for withdrawal of consent. In some cases this is stated explicitly in the Act, in others withdrawal of consent is not prohibited. Many embody the principle that consent to use the information only lasts until the purposes, for which the information was collected, have been met. For example, the provinces all require that if research is approved by a research ethics board under the Act, the information may only be used for the research specifically stated, and not for some other purpose.

In focus group discussions, consumers were largely unaware they could alter or withdraw consent; however, on completing the sessions many indicated they would consider doing so from now on. Once the implications of providing consent became clear, consumers did appear to want to have this right. Some legislation specifically provides for this under certain circumstances. Most stakeholders would also recommend that this right be extended, but others are concerned with the administrative implications this would entail, particularly for research.

> **Recommendation 5:** Allow consumers the right to make limits to any consent, clearly explain and promote this right, along with the potential risks and consequences of such limits.
>
> **Recommendation 6:** Give consideration to whether it would be viable to have consumers fill out a form (initiated by the health care system) to reconfirm consent choices, perhaps annually. This could eventually develop into a consent "profile" which would afford a wider range of choices available to the consumers, and assist in keeping records of what disclosures are made of information about a particular individual. If a consent profile model were developed, it would facilitate consumers changing consent when their information needs changed, and increase their ease of access to records containing their personal health information. There would be advantages to the health care system from this as well, by avoiding piecemeal record keeping and ensuring clear proof that legislated requirements regarding privacy are being met. The development of such a consent profile would have to be extremely carefully considered itself, to review the privacy implications of its use.

6.5 Data retention

As mentioned above, there is internal consistency among some of the statutes, which provide for the retention of data until the authorized purposes have been achieved.

Stakeholder groups are divided in their view between researchers and others. Researchers want to retain data indefinitely, in case it is useful for a currently unidentified purpose.

Others say that data should only be retained until the authorized purposes have expired or have been fulfilled. It is a debate about access vs. control. The balance between these two extreme positions likely shifts depending on the sensitivity of the personal health information. It also depends on who is making the decision about where the balance point is.

It is noteworthy that consumers have a different level of comfort for uses of identified and de-identified information, with the former warranting much closer personal control than the latter. When there is a proposed new use for the information, consumers want to be reintroduced to the process. They recognize that it may not be in the best interests of society for information to be destroyed; however, they want "to keep their fingers on" how their information will be used. It is thus important to ensure that consumers have the ability to reauthorize use of the same information for other purposes. Most of the consumers in the focus groups appeared to want the ability to tailor their consent to the specific use and as a function of the specific information requested. In other words, they seemed to support a profile-based layered consent model.

> **Recommendation 7:** Investigate the concept of introducing layered profiles of consent. The profiles could be maintained in a type of database that would make a layered approach to consent a workable concept for the health sector, taking an individual's wishes into account and comparing them to the proposed use. As well, those who do wish to have their information made available for research of all kinds could have their information identified as suitable to be used as a basic data source for preliminary surveys, pilot studies, etc. Evidently these ideas need to be researched and refined, but what is essential is that the technology that makes data protection so important could also be employed to make it individually tailored to a consumer's privacy concerns.

6.6 Data protection

Safeguards for personal health information are clearly needed; however, most consumers who addressed this issue in the context of this research consider the likelihood of a security breach regarding information in the health system to be no more and possibly even less probable than a security breach in another sector, such as banking. There is a long-standing trust in health care providers that extends to their commitment to protect consumers' personal health information, however, there is real concern for the human error that can occur in health information storage and transmission. The breaches discussed in the focus groups and in the surveys related to persons who inappropriately divulged or used information, not a data protection system that failed.

> **Recommendation 8:** Provisions of the relevant privacy Acts which require privacy processes to be established that put processes in place to enhance privacy and information security must be publicized, adhered to and enforced. Full systems

security is required, not just data protection in electronic or paper form, by for instance, providing front line staff with more sensitivity training and educating them about privacy responsibilities. One example of such provisions can be found in the *PIPEDA*, Principle 7 of Schedule 1, Safeguards. This is important because the whole health system is impugned when front line staff do not inspire confidence in their efforts to protect sensitive personal health information.

Recommendation 9: Conduct research that clarifies consumer views regarding varying levels of sensitivity of different health information. It is likely that there will be a general consensus about what personal health information is considered to be more sensitive than other personal health information. Analyze what the concerns are. This would provide input for establishing data protection standards for different types of health information, uses, disclosures and collection. This could be helpful to research ethics boards and the health system in general; the boards and health system would be apprised of the levels of protection consumers believe are required. Such research would further demonstrate that money invested in data protection systems is being well spent by enhancing institutions' ability to provide security.

Recommendation 10: Technological measures enhancing security and de-identifying health care information need further investigation.

6.7 Research

Research ethics boards are a feature of all the provincial Acts. They are not, however, constituted similarly or even tasked with the same functions in the different provinces. Some provincial Acts require them to be open and accountable to the public and some do not.

Recommendation 11: Introduce a mechanism for holding research ethics boards more accountable. Ideally a national, centralized registry, or accreditation process would be created. Alternatively, a list of accredited research ethics boards should be available to those who wish to pursue issues of research ethics board efficacy. Each province should insist that research ethics boards are transparent with regard to what issues they are deciding and what criteria they are using to make those decisions. As well, more basic information regarding how research ethics boards are constituted and approved, must be made known.

Recommendation 12: The rules for research ethics boards should be harmonized to the highest standard.-

6.8 Patient access to records

There is agreement among consumers and other stakeholder groups that individuals should have access to records containing their personal health information. This is also affirmed in the statutes reviewed. Consumers and other stakeholders also recognize that it is important for individuals to be able to determine who has already accessed these records. Several of the statutes note that patients should have access to the list of individuals and organizations that have accessed their records. Having access to such a list is important to consumers so that they may track the source of a breach, should a breach occur or be suspected.

Currently, many front-line health care providers do not seem to be aware that consumers have the right to access their records. The consumers participating in this research did not appear to be unaware of the rules and regulations that allow them access and thus are ill prepared to stand up for their rights. Legislation in most provinces provides that any fee for accessing information or copying records can be waived if individuals can demonstrate that paying for access would be a burden. This fact is virtually unknown, and certainly not effectively promoted.

> **Recommendation 13:** The health system needs to convey to consumers that they have a right to access, and that applicable fees can be waived. Specific rules for waiving fees should be established, but with an eye to ensuring that any process to waive fees is not itself invasive and provides a fair and consistent process for those who are economically disadvantaged. Fees should also be reasonable and justifiable given the time spent in providing access.
>
> **Recommendation 14:** Organizations and persons holding personal health information also need to record and promulgate how to access lists of who has had access to consumers' personal health information, so that erroneous information may be corrected. Again, the rules should be harmonized to the highest standard.

6.9 Link between correction of information and redress

Consumers need to be allowed to have their personal health information corrected in any file or database where it may be incorrect. At the same time they need to know all those who have previously accessed their records (and thus may have incorrect information). Consumers participating in this research and other stakeholders agree there should be an effective process for consumers to follow that ensures that erroneous data is corrected. All the statutes reviewed provide such a process, however some legislation stipulates that corrections are added to the record rather than replacing erroneous information. Such a provision is unlikely to be endorsed by most consumers, who want to have data changed rather than objections added. There are also varying levels of transparency required in the different statutes for the correction process. The statutes reviewed all include provisions for the process of correction, but with varying degrees of openness.

Recommendation 15: Inform individuals, where there is a process in place, how they can ensure that corrections are made to records containing personal health information. Where the process is not precise, or equivalent to other jurisdictions, it should be enhanced.

Recommendation 16: Investigate the feasibility of enhancing the portability of individuals' records, so that they can control information directly by moving information to a new physician, for example.

6.10 Redress

Consumers and other stakeholders agree that there should be a process to ensure that access has been appropriately granted and other compliance factors can be challenged. All the legislation reviewed provides for such redress. Nevertheless, this research suggest that consumers are unaware of the redress options available to them. Many don't know that the Privacy Commissioner exists, much less what his role in redress might be. Some are unaware of any recourse available to them, other than the prohibitive cost of hiring a lawyer.

Recommendation 17: Alert consumers to the existence of relevant commissioners or ombudsman offices and any other avenues of redress.

Recommendation 18: Outline a self-help "layered approach to redress". This would include such explanations as: how to talk to your doctor about privacy; how to make a complaint at the hospital; or how to decide to pursue the issue through other means. Then, determine how this approach could best be communicated to consumers, and by whom. This may be within the mandate of the Privacy Commissioner's office and/or the Commissioner's provincial counterparts.

6.11 In closing

There is no clear resolution to the dilemma of how to maintain an effective health care system that takes advantages of any efficiencies available from the burgeoning technology while respecting individuals' privacy. There may be benefits to information sharing, whether for individual patient file management, for research that might uncover new treatments, or for reviewing the health care system itself, but there is no clear way in which to measure those benefits that can be weighed against the equally difficult to assess value of privacy. Based on the research of consumer perspectives undertaken in the present study, consumers want to be asked for permission to use identified information about themselves. They want to be better informed as to how their information is to be used. They want to know their information is kept secure. They want to know their rights, obligations and alternatives. These are not impossible requests and can be addressed through changes in policies, practices and processes, both in the private sector and in government. Some of

these wishes are already provided for in legislation and thus only involve adherence to already existing rules.

Appendix A

Definitions (from the Acts) relating to Personal Health Information

Province/Act	Definitions Relating to Personal Health Information
Alberta – s.1(1)(k), (i),(o),(u)	**"health information"** means any or all of the following: (i) diagnostic, treatment and care information; (ii) health services provider information; (iii) registration information;".[1] … "**diagnostic, treatment and care information"** means information about any of the following: (i) the physical and mental health of an individual; (ii) a health service provided to an individual; (iii) the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance; (iv) a drug as defined in the Pharmaceutical Profession Act provided to an individual; (v) a health care aid, device, product, equipment or other item provided to an individual pursuant to a prescription or other authorization; (vi) the amount of any benefit paid or payable under the Alberta Health Care Insurance Act or any other amount paid or payable in respect of a health service provided to an individual, and includes any other information about an individual that is collected when a health service is provided to the individual, but does not include information that is not written, photographed, recorded or stored in some manner in a record;" (…) **"health services provider information"** means the following information relating to a health services provider: (i) name; (ii) business and home mailing addresses and electronic addresses; (iii) business and home telephone numbers and facsimile numbers; (iv) gender; (v) date of birth; (…) *(the definition continues, with accreditations completed, identifying number, restrictions on practice, etc)* **"registration information"** means information relating to an individual that falls within the following general categories and is more specifically described in the regulations: (i) demographic information, including the individual's personal health number; (ii) location information; (iii) telecommunications information; (iv) residency information; (v) health service eligibility information; (vi) billing information, but does not include information that is not written, photographed, recorded or stored in some manner in a record;
Manitoba s.1(1)	"**personal health information"** means recorded information about an identifiable individual that relates to (a) the individual's health, or health care history, including genetic information about the individual, (b) the provision of health care to the individual, or (c) payment for health care provided to the individual, and includes (d) the PHIN [Personal Health Identification Number] and any other identifying number, symbol or particular assigned to an individual, and

[1] Alberta, definitions,s.1(1)(k)

Province/Act	Definitions Relating to Personal Health Information
	(e) any identifying information about the individual that is collected in the course of, and is incidental to, the provision of health care or payment for health care"[2]
Ontario s.2	"**"personal health information"** means information in any form or manner about an individual, whether or not the information is recorded, if the information, (a) is information that, (i) identifies the individual, (ii) can be manipulated by a reasonably foreseeable method to identify the individual, or (iii) can be linked or matched by a reasonably foreseeable method to other information that identifies the individual or that can be manipulated by a reasonably foreseeable method to identify the individual, and (b) is information that, (i) relates to the physical or mental health of the individual, (ii) relates to the providing of health care to the individual, iii) is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual, (iv) relates to payments or eligibility for health care in respect of the individual, (v) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance, (vi) is the individual's health number, or (vii) identifies a provider of health care to the individual or a substitute decision-maker of the individual;"[3]
Saskatchewan s.2(m),(q)	**"personal health information"** means, with respect to an individual, whether living or deceased: (i) information with respect to the physical or mental health of the individual; (ii) information with respect to any health service provided to the individual; (iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual; (iv) information that is collected: (A) in the course of providing health services to the individual; or (B) incidentally to the provision of health services to the individual; or (v) registration information;[4] (…) **"registration information"** means information about an individual that is collected for the purpose of registering the individual for the provision of health services, and includes the individual's health services number and any other number assigned to the individual as part of a system of unique identifying numbers that is prescribed in the regulations;[5]
***PIPEDA* s.2(1)**	"**personal health information",** with respect to an individual, whether living or deceased, means (*a*) information concerning the physical or mental health of the individual; (*b*) information concerning any health service provided to the individual; (*c*) information concerning the donation by the individual of any body part or any bodily substance of the

[2] Manitoba Act, definitions, s.1(1)
[3] Ontario draft Act, s.2, definitions, "personal health information"
[4] Saskatchewan Act, definitions s.2(m)
[5] " (q)

Province/Act	Definitions Relating to Personal Health Information
	individual or information derived from the testing or examination of a body part or bodily substance of the individual; (*d*) information that is collected in the course of providing health services to the individual; or (*e*) information that is collected incidentally to the provision of health services to the individual." [6] (…) **"personal information"** means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."

[6] PIPEDA definitions, s.2(1)

Appendix B

Definitions for Organization, Trustee, or Custodian in the Acts reviewed

Act or Province	Definitions for "Organization", "Trustee" or "Custodian"
Alberta s.1(1)(f)	**"custodian"** means (i) the board of an approved hospital as defined in the Hospitals Act other than an approved hospital that is (A) owned and operated by a regional health authority established under the Regional Health Authorities Act, or (B) established and operated by the Alberta Cancer Board continued under the Cancer Programs Act; (ii) the operator of a nursing home as defined in the Nursing Homes Act other than a nursing home that is owned and operated by a regional health authority established under the Regional Health Authorities Act; (iii) a provincial health board established pursuant to regulations made under section 18(1)(a) of the Regional Health Authorities Act; (iv) a regional health authority established under the Regional Health Authorities Act; (v) a community health council as defined in the Regional Health Authorities Act; (vi) a subsidiary health corporation as defined in the Regional Health Authorities Act; (vii) the Alberta Cancer Board continued under the Cancer Programs Act; (viii) a board, council, committee, commission, panel or agency that is created by a custodian referred to in subclauses (i) to (vii), if all or a majority of its members are appointed by, or on behalf of, that custodian, but does not include a committee that has as its primary purpose the carrying out of quality assurance activities within the meaning of section 9 of the Alberta Evidence Act; (ix) a health services provider who is paid under the Alberta Health Care Insurance Plan to provide health services; (x) a licensed pharmacy as defined in the Pharmaceutical Profession Act; (xi) a pharmacist as defined in the Pharmaceutical Profession Act; (xii) the Department; (xiii) the Minister; (xiv) an individual or board, council, committee, commission, panel, agency or corporation designated in the regulations as a custodian; but does not include (xv) the Alberta Alcohol and Drug Abuse Commission continued under the Alcohol and Drug Abuse Act, or (xvi) a Community Board or a Facility Board, as those terms are defined in the Persons with Developmental Disabilities Community Governance Act;
Manitoba s.1(1)	**"trustee"** means a health professional, health care facility, public body, or health services agency that collects or maintains personal health information. "**health care facility**" means (a) a hospital, (b) a personal care home, © a psychiatric facility, (d) a medical clinic, (e) a laboratory, (f) The Manitoba Cancer Treatment and Research Foundation, and (g) a community health centre or other facility in which health care is provided and that is designated in the regulations; **"health professional**" means a person who is licensed or registered to provide health care under an Act of the Legislature or who is a member of a class of persons designated as health professionals in the regulations;

Act or Province	Definitions for "Organization", "Trustee" or "Custodian"
	"health services agency" means an organization that provides health care such as community or home-based health care pursuant to an agreement with another trustee; **"public body"** means a public body as defined in The Freedom of Information and Protection of Privacy Act, and for the purpose of this definition, the definitions of "department", "educational body", "government agency", "health care body", "local government body" and "local public body" in that Act apply;
Ontario **s.2**	**"organization"** includes a person, an association whether or not incorporated, a partnership, a health information custodian, a trade union and an individual, other than an individual acting in a personal and non-commercial capacity; **"health information custodian"** means, subject to section 3, a person described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with performing the person's powers or duties or the work described in the paragraph, if any: 1. A health care practitioner. 2. A service provider within the meaning of the Long-Term Care Act, 1994 who provides a service to which that Act applies. 3. A person who operates one of the following facilities, programs or services: i. A hospital within the meaning of the Public Hospitals Act, a private hospital within the meaning of the Private Hospitals Act, a psychiatric facility within the meaning of the Mental Health Act, an institution within the meaning of the Mental Hospitals Act, a regional cancer centre or an independent health facility within the meaning of the Independent Health Facilities Act. ii. An approved charitable home for the aged within the meaning of the Charitable Institutions Act, a home or joint home within the meaning of the Homes for the Aged and Rest Homes Act, a nursing home within the meaning of the Nursing Homes Act or a retirement home for elderly persons. iii. A pharmacy within the meaning of Part VI of the Drug and Pharmacies Regulation Act. iv. A laboratory or a specimen collection centre as defined in section 5 of the Laboratory and Specimen Collection Centre Licensing Act. v. An ambulance service within the meaning of the Ambulance Act. vi. A home for special care within the meaning of the Homes for Special Care Act. vii. A community health facility, program or service. 4. An evaluator within the meaning of the Health Care Consent Act, 1996 or an assessor within the meaning of t he Substitute Decisions Act, 1992. 5. A medical officer of health or a board of health within the meaning of the Health Protection and Promotion Act. 6. The Minister together with the Ministry of Health and Long-Term Care. 7. A prescribed person who compiles and maintains a registry or repository of, i. personal health information for the primary purpose of data analysis or research, ii. personal health information that relates to a specific disease or condition or that relates to the storage or donation of body parts or bodily substances. 8. A prescribed class of persons described in paragraph 7. 9. Any other person prescribed as a health information custodian if the person has custody or control of personal health information as a result of or in connection with performing prescribed powers, duties or work. 10. Any other prescribed class of persons described in paragraph 9;
Sask-atchewan **s.2(t)**	**"trustee"** means any of the following that have custody or control of personal health information: (i) a government institution; (ii) a district health board or an affiliate; (iii) a person who operates a special-care home as defined in The Housing and Special-care Homes Act; (iv) a licensee as defined in The Personal Care Homes Act; (v) a person who operates a facility as defined in The Mental Health Services Act;

Act or Province	Definitions for "Organization", "Trustee" or "Custodian"
	(vi) a licensee as defined in The Health Facilities Licensing Act; (vii) an operator as defined in The Ambulance Act; (viii) a licensee as defined in The Medical Laboratory Licensing Act, 1994; (ix) a proprietor as defined in The Pharmacy Act, 1996; (x) a community clinic: (A) as defined in section 263 of The Co-operatives Act, 1996; (B) within the meaning of section 9 of The Mutual Medical and Hospital Benefit Associations Act; or © incorporated or continued pursuant to The Non-profit Corporations Act, 1995; (xi) the Saskatchewan Cancer Foundation; (xii) a person, other than an employee of a trustee, who is: (A) a health professional licensed or registered pursuant to an Act for which the minister is responsible; or (B) a member of a class of persons designated as health professionals in the regulations; (xiii) a health professional body that regulates members of a health profession pursuant to an Act; (xiv) a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee; (xv) any other prescribed person, body or class of persons or bodies;
PIPEDA s.2(1)	**"organization"** includes an association, a partnership, a person and a trade union."

Appendix C

C.1 Focus Group Facilitation Materials

a. Moderator's guide
b. Backgrounder for the Moderator
c. Handouts for Focus Group participants

C.2 Consumer Survey

Note several versions of the survey were used depending on whether ascii-based email or PDF software were available to the respondent, whether the survey was completed by focus group members in a round table setting or whether it was sent by mail to newspaper ad respondents. The questions did not change but the formatting and some of the initial instructions varied slightly. The version presented here is that completed by Focus Group participants.

The Consumers' Association of Canada and the Public Interest Advocacy Centre

Privacy and Personal Health Information Draft Moderator's Guide for Focus Group Sessions

Topics to Cover	Timing
1. Introduction a) Round table introductions b) Focus group directions/ morning schedule a) Refer to moderator's backgrounder for background to project	15 minutes
2. Awareness – unaided a) What does privacy mean to you? – *5 minutes* b) What do you consider to be your Personal Health Information? *Brainstorm – 5 minutes* c) How much do you know about how your PHI is protected? Where did you hear it, what do you know? *Roundtable discussion – 10 minutes* **HANDOUT 1: Provide terminology (types of PHI - 2 minutes) Go over and make sure distinction between identified and de-identified information is clear)* d) Who currently has access to your PHI (both with and without your express consent)? Why? – *10 minutes* **HANDOUT 2: Some individuals and groups who currently hve or want access to your PHI?*	35 minutes (Running total: 50 minutes)
3. Consent a) Do you usually read any consent forms you have signed in the past dealing with your PHI? *Show of hands, invite participants to share examples – 5* minutes b) Have you ever been asked to give consent for your information to be shared for secondary purposes? When you give consent for treatment, are you also giving consent for the sharing of your PHI? How do you feel about this? *Roundtable discussion – 10 minutes*	30 minutes (Running total: 1 h 20 minutes)

Topics to Cover	Timing
c) Invite participants to consider the following example: *Scenario of pregnant mother who has miscarriage – 5 minutes* d) What are some of the advantages and disadvantages to blanket consent to PHI (Blanket: total access by secondary agencies to PHI) *Brainstorm 5-10 minutes*	
Break – refreshments	15 minutes
4. Redress a) Have you ever had a breach of confidentiality in the context of your personal health information? b) What would you do if you were to experience a breach of confidentiality regarding your PHI? Where would you turn? *Group discussion – 10 minutes*	10 minutes (Running total: 1 h 45 minutes)
5. Third Party Access a) Invite participants to consider the following scenario: *Researcher is denied access to PHI which may be helpful for advancing research knowledge (and/or need for Canadian based accident statistics) – 5 minutes* b) What are the consequences of not assuming any consent for release of PHI? (e.g., cannot use PHI without explicit consent) *10 minutes.* *(Be sure to make clear that often consent is needed for old data, years after its original collection.)*	15 minutes (Running total: 2 h)
6. Closing a) Summarize findings b) Ask respondents to indicate how aware they were of issues surrounding PHI before the focus group? (scale 0-10 and comments) **HANDOUT 3: Provide handout to participants regarding CAC summary principles and link to website (CAC main site).* c) Thank participants – remind them of the value they have provided, and how this information will be used d) Ask participants to fill out paper and pencil survey *(Make sure to warn them that the survey asks some detailed questions with regard to this issue, so they need to read each question carefully and ask if anything is unclear)*	15 minutes (Running total: 2 h 15 minutes)

Background Information for the Moderator

This information is provided so you will feel comfortable with the rationale behind the project and understand the context for the information we hope to elicit from participants. Please feel free in the introduction to share information from sections 1 to 3 with the participants. More detailed information should only be introduced where indicated in the moderator's guide as we are initially interested in what consumers think in the absence of information you provide.

1. What is the Consumers' Association of Canada (CAC)?

CAC, founded in 1947, is an independent, not-for-profit, volunteer-based, charitable organization. It's mandate is to inform and educate consumers on marketplace issues, to advocate for consumers with government and industry, and work with government and industry to solve marketplace problems. CAC focuses its work in the areas of food, health, trade, standards, financial services, communications industries and other marketplace issues as they emerge. It's mission is to represent and articulate the best interests of Canadian consumers to all levels of government and to all sectors of society by continually earning recognition as the trusted voice of the consumer on a national basis.

A national volunteer organization, CAC maintains a national secretariat in Ottawa with regional offices in Vancouver, Edmonton, Saskatoon, Winnipeg and Montreal.

2. What is the Public Interest Advocacy Centre (PIAC)?

The Public Interest Advocacy Centre (PIAC) is a non-profit federally incorporated organization. PIAC seeks to advance the interests of individuals and groups who are generally un-represented or underrepresented in issues of major public concern. We champion those issues that involve the delivery of important public and utility services. The Centre seeks to ensure that the public interest is served, and not neglected, by decision makers in government and the private sector when decisions are made about consumer issues. The Centre undertakes solid legal and research services on behalf of consumers. The Centre focuses primarily on consumer issues concerning telecommunications, energy, privacy, the information highway, electronic commerce, financial services, broadcasting, and competition law.

3. Why have CAC and PIAC organized this focus group?

CAC and PIAC are collaborating on a project entitled "Privacy and Health Information" in the context of a growing concern over whether the personal health information (PHI) of Canadian consumers of health services is being adequately protected in the wake of major changes to how such information is stored, shared and accessed. The final report will be submitted to the

Office of Consumer Affairs in Industry Canada, which is sponsoring this project. These focus groups are one of two main vehicles for directly tapping Canadian consumer views on at least some of the core issues in this debate.

4. What is the legal framework for these issues?

Some provinces, such as Alberta and Manitoba, have passed provincial legislation designed to protect personal information, including personal health information. Others, such as Ontario, have made an attempt, but to date have no legislation in place. The federal government extended the Personal Information Protection and Electronic Documents Act to include health information as of January 2002, but it is still not clear whether this will ensure adequate protection. Indeed it remains muddy which legislation applies where and in what cases. In all of this there has been a noticeable lack of input from the consumer as to what are, in their view, the key issues. These focus groups hope to remedy that oversight, at least to some extent.

5. What do CAC and PIAC want to learn from focus group attendees?

The question of privacy of PHI is a highly complex one, as is evident by the lack of consensus that emerged from the Privacy Working Group struck last year by Health Canada to address health sector concerns about the new Federal legislation. We cannot hope to address all the issues in this project, let alone in a focus group. It is important to keep in mind that the information that emerges from the focus groups will be used to complement a written survey that is currently being circulated across Canada. Most fundamentally, we are interested in:

- What to Canadian consumers understand by personal health information?
- What does privacy mean to them in this context?
- Have Canadians been thinking about the privacy of their personal health information (is this an issue on their radar)?
- For those that have, what are their experiences, concerns and fears?
- For those who have not, now that they are aware of the issues involved, what are their concerns and fears?
- to what extent are consumers comfortable with the sharing of the PHI and in what form?
- where do they stand on the inevitable tension between the sharing of information for the betterment of society and protection of information to ensure their privacy?

To that end, they will need to know that a distinction can be made between:

- health information that is **identified** (includes information that clearly identifies the individual) vs. **de-identified** information (information that has purportedly been stripped of all information that can be used to identify the individual). How successful de-identification can be is a matter of some debate.

- consent to the use of (personal) health information that is **explicit** (written or oral, with the purpose of the use outlined) vs. consent that is **implicit**, in which by their actions, individuals imply consent (e.g. by going to a doctor for treatment, individuals imply the release of information regarding what sort of treatment was provided to the provincial health insurance body, so the doctor can be paid. Much of the current system works on implicit consent.

  The OMA definitions for each are:

  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.

  Implied consent arises when 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.

- **primary uses** of PHI, in which the goal is the care and betterment of the individual to whom the information belongs and **secondary uses** of PHI, which can range from academic research, epidemiology to audit and evaluation of health services and even commercial uses of PHI.

6. How will the results from the focus groups be used?

The more detailed, nuanced reflections that emerge in the focus groups will be combined with a broader "take" on many of the same issues elicited through the email survey (copy attached). These findings will help define which among the myriad of issues relating to the privacy of health information are a priority for Canadian consumers and what they would like to see in terms of privacy safeguards. This will then be embedded in a detailed examination of federal and provincial legislation to see where gaps exist and what remedies may be suitable.

Handout #1: Personal Health Information and Privacy

Useful Terminology

Personal Health information (PHI) – This can include medical records, results of tests, diagnoses, number of visits to specialists/hospitals, tissue samples provided, but also factors which may be thought to determine your health such as education, lifestyle, income, eligibility for insurance, etc. Please think of personal health information in this broad way.

PHI can be :

A. Identified - information that is **directly** identifiable as yours (e.g., by including name, address etc.); OR

B.. De-identified[7] - information that may be **indirectly** identified as yours (e.g., by linking the information to information in other databases); OR,

- 'C' information that would be very hard to identify as yours (e.g. where the information is stored or shared only after having been combined with many other individuals' information, such as in total number of 'flu' cases treated in the month of February).

Explicit (or express) consent – when you are asked to sign a form (such as upon entry into a hospital) or when you are asked directly to grant consent to a health care provider for a particular procedure, treatment (can sometimes be oral). Explicit consent is unequivocal and does not require any inference on the part of the provider asking consent.

Implicit consent – when the actions you have taken implies or leads the person to believe you would have given consent if asked (for example, if you go to see a specialist who requires payment from your provincial insurance company, he may assume that you have given implied consent for him to disclose what treatment he gave you in order to receive payment).

[7] Participants should note that there is considerable debate regarding whether any PHI can truly be de-identified as it has been demonstrated that with the right technology, even de-identified information can be linked through several databases to identify specific individuals with high rates of accuracy. De-identified PHI that is thought to be safe from re-identification is sometimes called "anonymized" data (i.e. "C" in this list). In this focus group we do not distinguish between B and C .

Handout #2:

Personal Health Information (PHI) and Privacy

Some individuals or groups who currently have or want access to your PHI

Who has/wants access?	Why? (for example)
Your family physician	To provide you with primary health care
Hospital staff	To provide you with primary health care
Administrative decision-makers	To aid decision-making
Government	To better formulate health policies
Pharmaceutical companies	To aid in researching and developing new drugs
Private companies	Information used in genetic research to develop and produce products to sell in the marketplace a private firm selling products that may be useful to you, given your condition
Health Researchers	studying your disease a researcher studying a similar but unrelated disease a researcher looking at how frequently your condition is found across Canada
Family and friends	Any information provided by your physician to your family and friends because they can help or support you
Independent evaluators	an independent evaluator who is checking up on health care services being delivered in your province
Private or public insurance companies	In order to determine what fees are covered by your insurance
Your pharmacist	To aid in providing you with information about your prescription
Other health care workers	To aid a home care worker who has been assigned to help you while you recover
A specialist	To provide advice in diagnosing or treating your health problem

Note: This list is not meant to be exhaustive, but rather a guide as to how widespread interest in your PHI may be. Other entities who may have access to your PHI include your employer,

various government departments (e.g., Stats Can), lawyers and the court system. Can you think of any more?

Consumers' Association of Canada – Principles for Consumer Protection of Personal Health Information

Principles 1. Accountability

An organization, through its health information custodian, is responsible for maintaining confidentiality of the consumer's health information and ensuring proper procedures for the release of health information to third party sources.

Principle 2. Identifying Purposes

At the time of collection, the consumer will be informed of the purpose(s) for the health information being collected. Use of the information for other purposes requires the written consent of the consumer.

Principle 3. Consent

The collection and use of information may be for two types of purposes:
Primary purposes: The consumer seeks health care services within a therapeutic context. Personal health information is used or shared between health care providers for the ongoing care or treatment of the consumer.
Secondary purposes: Health information custodians and third parties which to collect, use, disclose, and access the consumer's health information for purposes other than originally identified shall have the written consent of the consumer.

Principle 4. Limiting Collection

The collection of information shall be limited to that which is necessary for the purpose(s) of providing health care products or services that the consumer is seeking.

Principle 5. Limiting Use and Disclosure

After obtaining the consumer's consent, the consumer's health information will not be used or disclosed for purpose(s) other than those for which it was collected, except when required by law, when ordered by a court of law, or when not to do so would put the consumer or others at grave risk.
The information custodian shall make all information anonymous for secondary uses. The consumer shall be informed of the information that has been disclosed to who the information was disclosed and for what purpose the information was used.

Principle 6. Limiting Storage

Health service providers may keep health records stored indefinitely for purposes of providing future services to the consumer or his/her descendants. In all other cases, the health information shall be retained only as long as necessary for the fulfillment of the purpose(s) for which it was collected, then shall be destroyed, erased, or made anonymous.

Principle 7. Accuracy

The consumer's health information shall be accurate, complete, and as up-to-date as necessary for the purposes for which it is used.

Principle 8. Safeguards

Safeguards shall be in accordance with the highest industry standards and practices. Effective security safeguards shall protect health information.

Principle 9. Transparency and Openness

The information custodian must provide the consumer, without undue delay and at no cost to the consumer, requested information on the policies and practices of the organization in maintaining and protecting personal health information.

Principle 10. Complaint, Dispute and Resolution Mechanism

The information custodian and/or organization shall have a complaint process that is easy to access and use. Consumers shall be informed of the complaint process. All complaints shall be investigated and, where justified, addressed to the satisfaction of the consumer.

Appendix B
Definitions for Organization, Trustee, or Custodian in the Acts reviewed

Act or Province	Definitions for "Organization", "Trustee" or "Custodian"
Alberta s.1(1)(f)	**"custodian"** means (i) the board of an approved hospital as defined in the Hospitals Act other than an approved hospital that is (A) owned and operated by a regional health authority established under the Regional Health Authorities Act, or (B) established and operated by the Alberta Cancer Board continued under the Cancer Programs Act; (ii) the operator of a nursing home as defined in the Nursing Homes Act other than a nursing home that is owned and operated by a regional health authority established under the Regional Health Authorities Act; (iii) a provincial health board established pursuant to regulations made under section 18(1)(a) of the Regional Health Authorities Act; (iv) a regional health authority established under the Regional Health Authorities Act; (v) a community health council as defined in the Regional Health Authorities Act; (vi) a subsidiary health corporation as defined in the Regional Health Authorities Act; (vii) the Alberta Cancer Board continued under the Cancer Programs Act; (viii) a board, council, committee, commission, panel or agency that is created by a custodian referred to in subclauses (i) to (vii), if all or a majority of its members are appointed by, or on behalf of, that custodian, but does not include a committee that has as its primary purpose the carrying out of quality assurance activities within the meaning of section 9 of the Alberta Evidence Act; (ix) a health services provider who is paid under the Alberta Health Care Insurance Plan to provide health services; (x) a licensed pharmacy as defined in the Pharmaceutical Profession Act; (xi) a pharmacist as defined in the Pharmaceutical Profession Act; (xii) the Department; (xiii) the Minister; (xiv) an individual or board, council, committee, commission, panel, agency or corporation designated in the regulations as a custodian; but does not include (xv) the Alberta Alcohol and Drug Abuse Commission continued under the Alcohol and Drug Abuse Act, or (xvi) a Community Board or a Facility Board, as those terms are defined in the Persons with Developmental Disabilities Community Governance Act;
Manitoba s.1(1)	**"trustee"** means a health professional, health care facility, public body, or health services agency that collects or maintains personal health information. "**health care facility**" means (a) a hospital, (b) a personal care home, © a psychiatric facility, (d) a medical clinic, (e) a laboratory, (f) The Manitoba Cancer Treatment and Research Foundation, and (g) a community health centre or other facility in which health care is provided and that is designated in the regulations; **"health professional**" means a person who is licensed or registered to provide health care under an Act of the Legislature or who is a member of a class of persons designated as health professionals in the regulations; **"health services agency"** means an organization that provides health care such as community or home-based health care pursuant to an agreement with another trustee;

Act or Province	Definitions for "Organization", "Trustee" or "Custodian"
	"public body" means a public body as defined in The Freedom of Information and Protection of Privacy Act, and for the purpose of this definition, the definitions of "department", "educational body", "government agency", "health care body", "local government body" and "local public body" in that Act apply;
Ontario s.2	**"organization"** includes a person, an association whether or not incorporated, a partnership, a health information custodian, a trade union and an individual, other than an individual acting in a personal and non-commercial capacity; **"health information custodian"** means, subject to section 3, a person described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with performing the person's powers or duties or the work described in the paragraph, if any: 1. A health care practitioner. 2. A service provider within the meaning of the Long-Term Care Act, 1994 who provides a service to which that Act applies. 3. A person who operates one of the following facilities, programs or services: i. A hospital within the meaning of the Public Hospitals Act, a private hospital within the meaning of the Private Hospitals Act, a psychiatric facility within the meaning of the Mental Health Act, an institution within the meaning of the Mental Hospitals Act, a regional cancer centre or an independent health facility within the meaning of the Independent Health Facilities Act. ii. An approved charitable home for the aged within the meaning of the Charitable Institutions Act, a home or joint home within the meaning of the Homes for the Aged and Rest Homes Act, a nursing home within the meaning of the Nursing Homes Act or a retirement home for elderly persons. iii. A pharmacy within the meaning of Part VI of the Drug and Pharmacies Regulation Act. iv. A laboratory or a specimen collection centre as defined in section 5 of the Laboratory and Specimen Collection Centre Licensing Act. v. An ambulance service within the meaning of the Ambulance Act. vi. A home for special care within the meaning of the Homes for Special Care Act. vii. A community health facility, program or service. 4. An evaluator within the meaning of the Health Care Consent Act, 1996 or an assessor within the meaning of t he Substitute Decisions Act, 1992. 5. A medical officer of health or a board of health within the meaning of the Health Protection and Promotion Act. 6. The Minister together with the Ministry of Health and Long-Term Care. 7. A prescribed person who compiles and maintains a registry or repository of, i. personal health information for the primary purpose of data analysis or research, ii. personal health information that relates to a specific disease or condition or that relates to the storage or donation of body parts or bodily substances. 8. A prescribed class of persons described in paragraph 7. 9. Any other person prescribed as a health information custodian if the person has custody or control of personal health information as a result of or in connection with performing prescribed powers, duties or work. 10. Any other prescribed class of persons described in paragraph 9;
Sask-atchewan **s.2(t)**	**"trustee"** means any of the following that have custody or control of personal health information: (i) a government institution; (ii) a district health board or an affiliate; (iii) a person who operates a special-care home as defined in The Housing and Special-care Homes Act; (iv) a licensee as defined in The Personal Care Homes Act; (v) a person who operates a facility as defined in The Mental Health Services Act; (vi) a licensee as defined in The Health Facilities Licensing Act; (vii) an operator as defined in The Ambulance Act; (viii) a licensee as defined in The Medical Laboratory Licensing Act, 1994;

Act or Province	Definitions for “Organization”, “Trustee” or “Custodian”
	(ix) a proprietor as defined in The Pharmacy Act, 1996; (x) a community clinic: (A) as defined in section 263 of The Co-operatives Act, 1996; (B) within the meaning of section 9 of The Mutual Medical and Hospital Benefit Associations Act; or © incorporated or continued pursuant to The Non-profit Corporations Act, 1995; (xi) the Saskatchewan Cancer Foundation; (xii) a person, other than an employee of a trustee, who is: (A) a health professional licensed or registered pursuant to an Act for which the minister is responsible; or (B) a member of a class of persons designated as health professionals in the regulations; (xiii) a health professional body that regulates members of a health profession pursuant to an Act; (xiv) a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee; (xv) any other prescribed person, body or class of persons or bodies;
PIPEDA s.2(1)	**“organization”** includes an association, a partnership, a person and a trade union.”

Appendix C

C.1 Focus Group Facilitation Materials

a. Moderator's guide
b. Backgrounder for the Moderator
c. Handouts for Focus Group participants

C.2 Consumer Survey

Note several versions of the survey were used depending on whether ascii-based email or PDF software were available to the respondent, whether the survey was completed by focus group members in a round table setting or whether it was sent by mail to newspaper ad respondents. The questions did not change but the formatting and some of the initial instructions varied slightly. The version presented here is that completed by Focus Group participants.

The Consumers' Association of Canada and the Public Interest Advocacy Centre

Privacy and Personal Health Information Draft Moderator's Guide for Focus Group Sessions

Topics to Cover	Timing
1. Introduction a) Round table introductions b) Focus group directions/ morning schedule a) Refer to moderator's backgrounder for background to project	15 minutes
2. Awareness – unaided a) What does privacy mean to you? – *5 minutes* b) What do you consider to be your Personal Health Information? *Brainstorm – 5 minutes* c) How much do you know about how your PHI is protected? Where did you hear it, what do you know? *Roundtable discussion – 10 minutes* **HANDOUT 1: Provide terminology (types of PHI - 2 minutes) Go over and make sure distinction between identified and de-identified information is clear)* d) Who currently has access to your PHI (both with and without your express consent)? Why? – *10 minutes* **HANDOUT 2: Some individuals and groups who currently hve or want access to your PHI?*	35 minutes (Running total: 50 minutes)
3. Consent a) Do you usually read any consent forms you have signed in the past dealing with your PHI? *Show of hands, invite participants to share examples – 5* minutes b) Have you ever been asked to give consent for your information to be shared for secondary purposes? When you give consent for treatment, are you also giving consent for the sharing of your PHI? How do you feel about this? *Roundtable discussion – 10 minutes* c) Invite participants to consider the following example: *Scenario of pregnant mother who has miscarriage – 5 minutes*	30 minutes (Running total: 1 h 20 minutes)

Topics to Cover	Timing
d) What are some of the advantages and disadvantages to blanket consent to PHI (Blanket: total access by secondary agencies to PHI) *Brainstorm 5-10 minutes*	
Break – refreshments	15 minutes
4. Redress a) Have you ever had a breach of confidentiality in the context of your personal health information? b) What would you do if you were to experience a breach of confidentiality regarding your PHI? Where would you turn? *Group discussion – 10 minutes*	10 minutes (Running total: 1 h 45 minutes)
5. Third Party Access a) Invite participants to consider the following scenario: *Researcher is denied access to PHI which may be helpful for advancing research knowledge (and/or need for Canadian based accident statistics) – 5 minutes* b) What are the consequences of not assuming any consent for release of PHI? (e.g., cannot use PHI without explicit consent) *10 minutes.* *(Be sure to make clear that often consent is needed for old data, years after its original collection.)*	15 minutes (Running total: 2 h)
6. Closing a) Summarize findings b) Ask respondents to indicate how aware they were of issues surrounding PHI before the focus group? (scale 0-10 and comments) **HANDOUT 3: Provide handout to participants regarding CAC summary principles and link to website (CAC main site).* c) Thank participants – remind them of the value they have provided, and how this information will be used d) Ask participants to fill out paper and pencil survey *(Make sure to warn them that the survey asks some detailed questions with regard to this issue, so they need to read each question carefully and ask if anything is unclear)*	15 minutes (Running total: 2 h 15 minutes)

Handout # 3 for Focus Group Participants: CAC Principles of PHI Protection

Background Information for the Moderator

This information is provided so you will feel comfortable with the rationale behind the project and understand the context for the information we hope to elicit from participants. Please feel free in the introduction to share information from sections 1 to 3 with the participants. More detailed information should only be introduced where indicated in the moderator's guide as we are initially interested in what consumers think in the absence of information you provide.

1. What is the Consumers' Association of Canada (CAC)?

CAC, founded in 1947, is an independent, not-for-profit, volunteer-based, charitable organization. It's mandate is to inform and educate consumers on marketplace issues, to advocate for consumers with government and industry, and work with government and industry to solve marketplace problems. CAC focuses its work in the areas of food, health, trade, standards, financial services, communications industries and other marketplace issues as they emerge. It's mission is to represent and articulate the best interests of Canadian consumers to all levels of government and to all sectors of society by continually earning recognition as the trusted voice of the consumer on a national basis.

A national volunteer organization, CAC maintains a national secretariat in Ottawa with regional offices in Vancouver, Edmonton, Saskatoon, Winnipeg and Montreal.

2. What is the Public Interest Advocacy Centre (PIAC)?

The Public Interest Advocacy Centre (PIAC) is a non-profit federally incorporated organization. PIAC seeks to advance the interests of individuals and groups who are generally un-represented or underrepresented in issues of major public concern. We champion those issues that involve the delivery of important public and utility services. The Centre seeks to ensure that the public interest is served, and not neglected, by decision makers in government and the private sector when decisions are made about consumer issues. The Centre undertakes solid legal and research services on behalf of consumers. The Centre focuses primarily on consumer issues concerning telecommunications, energy, privacy, the information highway, electronic commerce, financial services, broadcasting, and competition law.

3. Why have CAC and PIAC organized this focus group?

CAC and PIAC are collaborating on a project entitled "Privacy and Health Information" in the context of a growing concern over whether the personal health information (PHI) of Canadian consumers of health services is being adequately protected in the wake of major changes to how such information is stored, shared and accessed. The final report will be submitted to the Office of Consumer Affairs in Industry Canada, which is sponsoring this project. These focus groups are one of two main vehicles for directly tapping Canadian consumer views on at least some of the core issues in this debate.

4. What is the legal framework for these issues?

Some provinces, such as Alberta and Manitoba, have passed provincial legislation designed to protect personal information, including personal health information. Others, such as Ontario, have made an attempt, but to date have no legislation in place. The federal government extended the Personal Information Protection and Electronic Documents Act to include health information as of January 2002, but it is still not clear whether this will ensure adequate protection. Indeed it remains muddy which legislation applies where and in what cases. In all of this there has been a noticeable lack of input from the consumer as to what are, in their view, the key issues. These focus groups hope to remedy that oversight, at least to some extent.

5. What do CAC and PIAC want to learn from focus group attendees?

The question of privacy of PHI is a highly complex one, as is evident by the lack of consensus that emerged from the Privacy Working Group struck last year by Health Canada to address health sector concerns about the new Federal legislation. We cannot hope to address all the issues in this project, let alone in a focus group. It is important to keep in mind that the information that emerges from the focus groups will be used to complement a written survey that is currently being circulated across Canada. Most fundamentally, we are interested in:

- What to Canadian consumers understand by personal health information?
- What does privacy mean to them in this context?
- Have Canadians been thinking about the privacy of their personal health information (is this an issue on their radar)?
- For those that have, what are their experiences, concerns and fears?
- For those who have not, now that they are aware of the issues involved, what are their concerns and fears?
- to what extent are consumers comfortable with the sharing of the PHI and in what form?
- where do they stand on the inevitable tension between the sharing of information for the betterment of society and protection of information to ensure their privacy?

To that end, they will need to know that a distinction can be made between:

- health information that is **identified** (includes information that clearly identifies the individual) vs. **de-identified** information (information that has purportedly been

stripped of all information that can be used to identify the individual). How successful de-identification can be is a matter of some debate.

- consent to the use of (personal) health information that is **explicit** (written or oral, with the purpose of the use outlined) vs. consent that is **implicit**, in which by their actions, individuals imply consent (e.g. by going to a doctor for treatment, individuals imply the release of information regarding what sort of treatment was provided to the provincial health insurance body, so the doctor can be paid. Much of the current system works on implicit consent.

  The OMA definitions for each are:

  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.

  Implied consent arises when 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.

- **primary uses** of PHI, in which the goal is the care and betterment of the individual to whom the information belongs and **secondary uses** of PHI, which can range from academic research, epidemiology to audit and evaluation of health services and even commercial uses of PHI.

6. How will the results from the focus groups be used?

The more detailed, nuanced reflections that emerge in the focus groups will be combined with a broader "take" on many of the same issues elicited through the email survey (copy attached). These findings will help define which among the myriad of issues relating to the privacy of health information are a priority for Canadian consumers and what they would like to see in terms of privacy safeguards. This will then be embedded in a detailed examination of federal and provincial legislation to see where gaps exist and what remedies may be suitable.

Handout #1: Personal Health Information and Privacy

Useful Terminology

Personal Health information (PHI) – This can include medical records, results of tests, diagnoses, number of visits to specialists/hospitals, tissue samples provided, but also factors which may be thought to determine your health such as education, lifestyle, income, eligibility for insurance, etc. Please think of personal health information in this broad way.

PHI can be :

A. Identified - information that is **directly** identifiable as yours (e.g., by including name, address etc.); OR

B.. De-identified[1] - information that may be **indirectly** identified as yours (e.g., by linking the information to information in other databases); OR,

- 'C' information that would be very hard to identify as yours (e.g. where the information is stored or shared only after having been combined with many other individuals' information, such as in total number of 'flu' cases treated in the month of February).

Explicit (or express) consent – when you are asked to sign a form (such as upon entry into a hospital) or when you are asked directly to grant consent to a health care provider for a particular procedure, treatment (can sometimes be oral). Explicit consent is unequivocal and does not require any inference on the part of the provider asking consent.

Implicit consent – when the actions you have taken implies or leads the person to believe you would have given consent if asked (for example, if you go to see a specialist who requires payment from your provincial insurance company, he may assume that you have given implied consent for him to disclose what treatment he gave you in order to receive payment).

[1] Participants should note that there is considerable debate regarding whether any PHI can truly be de-identified as it has been demonstrated that with the right technology, even de-identified information can be linked through several databases to identify specific individuals with high rates of accuracy. De-identified PHI that is thought to be safe from re-identification is sometimes called "anonymized" data (i.e. "C" in this list). In this focus group we do not distinguish between B and C .

Handout #2:
Personal Health Information (PHI) and Privacy
Some individuals or groups who currently have or want access to your PHI

[can you get the column on the right to line up, Jennifer, I can't]

Who has/wants access?	Why? (for example)
Your family physician	To provide you with primary health care
Hospital staff	To provide you with primary health care
Administrative decision-makers	To aid decision-making
Government	To better formulate health policies
Pharmaceutical companies	To aid in researching and developing new drugs
Private companies	Information used in genetic research to develop and produce products to sell in the marketplace a private firm selling products that may be useful to you, given your condition
Health Researchers	studying your disease a researcher studying a similar but unrelated disease a researcher looking at how frequently your condition is found across Canada
Family and friends	Any information provided by your physician to your family and friends because they can help or support you
Independent evaluators	an independent evaluator who is checking up on health care services being delivered in your province
Private or public insurance companies	In order to determine what fees are covered by your insurance
Your pharmacist	To aid in providing you with information about your prescription
Other health care workers	To aid a home care worker who has been assigned to help you while you recover
A specialist	To provide advice in diagnosing or treating your health problem

Note: This list is not meant to be exhaustive, but rather a guide as to how widespread interest in your PHI may be. Other entities who may have access to your PHI include your employer, various government departments (e.g., Stats Can), lawyers and the court system. Can you think of any more?

Handout # 3 for Focus Group Participants: CAC Principles of PHI Protection

Consumers' Association of Canada – Principles for Consumer Protection of Personal Health Information

Principles 1. Accountability

An organization, through its health information custodian, is responsible for maintaining confidentiality of the consumer's health information and ensuring proper procedures for the release of health information to third party sources.

Principle 2. Identifying Purposes

At the time of collection, the consumer will be informed of the purpose(s) for the health information being collected. Use of the information for other purposes requires the written consent of the consumer.

Principle 3. Consent

The collection and use of information may be for two types of purposes:
Primary purposes: The consumer seeks health care services within a therapeutic context. Personal health information is used or shared between health care providers for the ongoing care or treatment of the consumer.
Secondary purposes: Health information custodians and third parties which to collect, use, disclose, and access the consumer's health information for purposes other than originally identified shall have the written consent of the consumer.

Principle 4. Limiting Collection

The collection of information shall be limited to that which is necessary for the purpose(s) of providing health care products or services that the consumer is seeking.

Principle 5. Limiting Use and Disclosure

After obtaining the consumer's consent, the consumer's health information will not be used or disclosed for purpose(s) other than those for which it was collected, except when required by law, when ordered by a court of law, or when not to do so would put the consumer or others at grave risk.
The information custodian shall make all information anonymous for secondary uses. The consumer shall be informed of the information that has been disclosed to who the information was disclosed and for what purpose the information was used.

Principle 6. Limiting Storage

Health service providers may keep health records stored indefinitely for purposes of providing future services to the consumer or his/her descendants. In all other cases, the health information shall be retained only as long as necessary for the fulfillment of the purpose(s) for which it was collected, then shall be destroyed, erased, or made anonymous.

Principle 7. Accuracy

The consumer's health information shall be accurate, complete, and as up-to-date as necessary for the purposes for which it is used.

Principle 8. Safeguards

Safeguards shall be in accordance with the highest industry standards and practices. Effective security safeguards shall protect health information.

Principle 9. Transparency and Openness

The information custodian must provide the consumer, without undue delay and at no cost to the consumer, requested information on the policies and practices of the organization in maintaining and protecting personal health information.

Principle 10. Complaint, Dispute and Resolution Mechanism

The information custodian and/or organization shall have a complaint process that is easy to access and use. Consumers shall be informed of the complaint process. All complaints shall be investigated and, where justified, addressed to the satisfaction of the consumer.

PERSONAL HEALTH INFORMATION AND YOUR PRIVACY
A Survey for the Consumers' Association of Canada (CAC) and The Public Interest Advocacy Centre (PIAC)

CAC is an independent, non-profit, volunteer-based charitable organization. Its mandate is to inform and educate consumers with regard to marketplace issues and to advocate on behalf of consumers with government and industry. **PIAC** is a non-profit organization that provides legal and research services on behalf of consumer interests concerning the provision of important public services.

CAC and PIAC have undertaken to poll Canadian consumer views on issues surrounding the privacy of personal health information. These issues affect all Canadians who will all likely be involved at some point with the Canadian health care system directly or indirectly, so we would ask that you take a few minutes to answer the questions below and share with us your thoughts, concerns and experiences. Please note that this survey is for Canadian respondents only.

All information collected in this survey will be treated **confidentially** and stored **anonymously**. Any specific examples drawn from comments made in the survey will be masked to ensure the individual is not identifiable. The final report will be available from CAC or PIAC.

Please complete this survey and pass to the moderator.

Note: As you now are aware this is a complicated issue. If any of the questions are unclear, please raise your hand and ask the moderator or his assistant for clarification.

Some of the questions below ask you to rate on a scale of 0 to 5 to what extent you are satisfied or concerned with the statements made. Please think of the scale as follows:

0.....1.....2.....3.....4.....5
not at all neutral or somewhat a great deal

The questions below deal with your PERSONAL HEALTH INFORMATION. This can include medical records, results of tests, diagnoses, number of visits to specialists/hospitals, tissue samples provided, but also factors which may be thought to determine your health such as education, lifestyle, income, eligibility for insurance, etc. Please think of personal health information in this broad way.

1. On the scale noted above, please rate to what extent are you concerned:

___ That others can access your personal health information without your permission

___ That others may be using your personal health information for purposes other than your health care

___ That the quality of your health care may be negatively affected if you restrict others' access to (and/or use of) your personal health information

___ That your personal health information may be made available by accident to individuals you believe should not have access to it

___ That your personal health information may be made available on purpose to individuals you believe should not have access to it

___ That the electronic databases in which your personal health information is stored may not be that secure

___ That paper records in which your personal health information is stored may not be that secure

___ That, even though your personal health information may be included in large databases without any identifying information, it may not be that difficult for someone to link that information with other databases and be able to identify you

2. (a) Have you ever had an experience in which the confidentiality of your personal health information was compromised? (yes or no) _____

(b) If yes, please explain [take as much room as you need]:

(c) If you are unaware of any specific instance, are you still concerned that the confidentiality of your personal health information may have been compromised at any point in the past? (yes or no) _____

(d) If yes, please explain [take as much room as you need]:

3. (a) Have you ever had an experience in which information about you was NOT made available to others who needed it? (yes or no) _____

(b) If yes, please explain [take as much room as you need]:

4. (a) Have you ever asked to access records about your own personal health information? (yes or no) _____

(If you answered no, skip to question 5.)

(b) Were you ever refused access? (yes or no) _____

(c) If you answered yes to 4 (b), what were the circumstances? [take as much room as you need]:

(d) If you asked for and obtained access to your personal health records, did you understand them? (yes or no) _____

(e) If you answered no to 4 (d), did you ask to have someone clarify or interpret the information for you? (yes or no) _____

(f) If you answered yes to 4 (e), was this done to your satisfaction? (yes or no) _____

(g) If you obtained access to your personal health records and found that information in them was inaccurate in your view, what action would you take? [take as much room as you need]:

(h) Have you ever held back information from a health professional because you did not want it in your file? (yes or no) _____

(j) If yes, what was the situation? [take as much room as you need]:

Remember the scale you are using

0.....1.....2.....3.....4.....5
not at all neutral or somewhat a great deal

5. For the next question, we would like you to imagine yourself in the following scenario (one, we hope, you will never have to experience in reality)

> *You have just been diagnosed with a blood disease. This disease means you must take time off work, sometimes need help around the house and require various medications. As you seek care, your personal health information becomes of interest to others.*

(a) Please indicate below if you think the following individuals and groups CAN currently access your (identified) information now WITHOUT asking for your consent (check any that apply):

____ a specialist called in to help on your case

____ a researcher studying your blood disease

____ a researcher studying a similar but unrelated blood disease

____ a drug company researching new drugs

____ a researcher looking at how frequently your condition is found across Canada

____ the private or public insurer paying for your treatment

____ an independent evaluator who is checking up on health care services being delivered in your province

____ a friend or family member who your doctor feels can help or support you

____ a home care worker who has been assigned to help you while you recover

____ a private firm selling products that may be useful to you, given your condition

____ a pharmacist filling your prescription

(b) Using the scale above, rate how comfortable you would be if these individuals and groups were allowed to access your IDENTIFIED personal health information WITHOUT asking for your consent. (Note: the list is the same as in (a)):

____ a specialist called in to help on your case

____ a researcher studying your blood disease

____ a researcher studying a similar but unrelated blood disease

____ a drug company researching new drugs

____ a researcher looking at how frequently your condition is found across Canada

____ the private or public insurer paying for your treatment

____ an independent evaluator who is checking up on health care services being delivered in your province

____ a friend or family member who your doctor feels can help or support you

____ a home care worker who has been assigned to help you while you recover

____ a private firm selling products that may be useful to you, given your condition

____ a pharmacist filling your prescription

6. There are rules that each of the above individuals and groups must follow to access or use your personal health information. These rules change depending on the circumstances. Part (a) asks what you think these rules are NOW, and part (b) asks what you think the rules SHOULD BE.

(a) Please indicate what you think the current requirements or rules are about consent. For each individual or group listed below, note whether you think that they currently are:

- required to ask for your consent (write R for required)
- allowed to assume you have given consent (write A for assume), or
- do not have to ask for or assume your consent at all (write N for no consent).

An example of **required consent would be when you are asked to sign a form upon admission to hospital that states clearly that you are giving permission to the hospital to treat your illness.

** An example of **assumed** consent would be when you go to your family doctor for a specific procedure, he may assume you are giving him permission to tell your provincial insurance company what procedure was done so that he can get paid.

____ a specialist called in to help on your case

____ a researcher studying your blood disease

____ a researcher studying a similar but unrelated blood disease

____ a drug company researching new drugs

____ a researcher looking at how frequently your condition is found across Canada

____ the private or public insurer paying for your treatment

____ an independent evaluator who is checking up on health care services being delivered in your province

____ a friend or family member who your doctor feels can help or support you

____ a home care worker who has been assigned to help you while you recover

____ a private firm selling products that may be useful to you, given your condition

____ a pharmacist filling your prescription

(b) In 6 (a) we asked you what sort of consent you think is CURRENTLY required in each case. In this question please indicated what sort of consent SHOULD BE required. For each individual or group listed below, please note below whether they should be:

- required to ask for your consent (write R for required)
- allowed to assume you have given consent (write A for assume), or
- should not have to ask for or assume your consent at all (write N for no consent).

____ a specialist called in to help on your case

____ a researcher studying your blood disease

____ a researcher studying a similar but unrelated blood disease

____ a drug company researching new drugs

____ a researcher looking at how frequently your condition is found across Canada

____ the private or public insurer paying for your treatment

____ an independent evaluator who is checking up on health care services being delivered in your province

____ a friend or family member who your doctor feels can help or support you

____ a home care worker who has been assigned to help you while you recover

____ a private firm selling products that may be useful to you, given your condition

____ a pharmacist filling your prescription

Remember the scale you are using

0……1……2……3……4……5
not at all neutral or somewhat a great deal

7. Suppose a medical form contained health information about you, but it was impossible to know that it was your personal health information because any identifying information (name, address, social insurance number) has been removed. Using the same scale we have been using

rate how comfortable you would be if information on the form was released WITHOUT your consent to:

____ a researcher studying your blood disease

____ a researcher studying a similar but unrelated blood disease

____ a drug company researching new drugs

____ a researcher looking at how frequently your condition is found across Canada

____ the private or public insurer paying for your treatment

____ an independent evaluator who is checking up on health care services being delivered in your province

____ a private firm selling products that may be useful to you, given your condition

____ a pharmacist filling your prescription

8 (a) Would you allow your personal health information to be used for research purposes in some circumstances?

Yes OR No _____

(b) If you answered yes to question 8 (a), imagine your doctor has asked for your consent to release your personal health information for a research project. Using the same scale we have been using (least 0..1..2..3..4..5 most) rate to what extent you would be comfortable giving your consent:

____ Where the research could not be done without your information
____ Where the research proposes to develop a remedy for a disease you or someone you love suffers from
____ Where you do not know what the research purposes are
____ Where you do not know who will benefit from the research
____ Where you have ethical objections to the methods used in the research
____ Where you feel the information needed is particularly sensitive

(c) Please indicate if there are other factors that may influence your decision whether to share your health information for research [take as much room as you need]:

(d) Have you ever wanted to withhold consent, but felt uncomfortable refusing the release of personal health information?

Yes OR No _____

(e) If yes, what was the situation? [take as much room as you need]:

9. (a) If you were to discover that your personal health information was being handled in a way that made you uncomfortable, where would you go currently to resolve the problem? [take as much room as you need]:

(b) Are you confident that the approach noted in 9 (a) would resolve the problem?

Yes OR No

Remember the scale you are using

0.....1.....2.....3.....4.....5
not at all neutral or somewhat a great deal

10. (a) On the same scale, to what extent are you satisfied with:

____ the amount of information you have received about health information and privacy (from any source)
____ the quality and usefulness of the information you have received about health information and privacy (from any source)

Finally we would like to ask you a few questions about yourself that will allow us to situate you within the larger Canadian population (but not identify you!). Please put an x in the appropriate box:

Age:

- ☐ under 20
- ☐ 20-39
- ☐ 40-59
- ☐ 60 +

Education:

Please indicate the highest level of studies **completed:**

- ☐ grade school
- ☐ high school
- ☐ technical/vocational school
- ☐ undergraduate university degree
- ☐ graduate/professional degree

Gender:

- ☐ M
- ☐ F

Field of work:

_____

Family: Are you actively caring for children? ☐ Yes ☐ No

Are you actively caring for an elderly person (parent, relative) ☐ Yes ☐ No

Province of residence _____

How did you hear about/find out about this survey?

Do you have any comments on this survey? [use the back, if necessary]:

APPENDIX D

Participants in the Study and their organizations:

1. **Authors of the study**

Consumers' Association of Canada (CAC) is a 55 year old independent, not-for-profit, volunteer based organization with a National office in Ottawa and provincial/Territorial Branches. Our mandate is to inform and educate consumers on market place issues, to advocate for consumers with government and industry, and to work with government and industry to solve market place problems in beneficial ways.

CAC focuses its work in the areas of health, food, trade, standards, financial services, communication services and other market place issues as they emerge. All CAC policies on specific issues are framed within a set of general consumer-oriented principles. Eight such principles govern consumer associations belonging to the worldwide federation of consumer groups, Consumers International. Among these principles are the right to choice, safety, information and a healthy environment.

Public Interest Advocacy Centre (PIAC) is a registered charitable organization federally incorporated in 1976. It provides legal advice, representation, and specialized research on a non-profit basis to groups and individuals who are voicing public concern, and who would otherwise not have access to such services. Since its inception, PIAC has made issues associated with the regulatory process a priority. In particular, the Centre has developed a reputation for providing effective advocacy in telecommunications, cable broadcasting, energy, transportation and privacy. Since 1992, PIAC has also become a membership organization. While it continues its role as counsel to membership-driven organizations in hearings and courtrooms, PIAC also plays a larger advocacy role at both formal proceedings and liaising with governments and other stake holders.

Kathleen Priestman joined the Public Interest Advocacy Centre in the spring of 2001 as a Research Analyst. Prior to joining PIAC, Kathleen worked as a research analyst for the Office of Consumer Affairs, Industry Canada. Her background in consumer issues includes work for the Law Centre in Victoria, BC, the Family Justice branch of the Ministry of the Attorney General, and the Ministry of Social Development and Economic Security, both in British Columbia. She is a graduate of the University of Victoria, where a B.A. in Linguistics (1994) led her to pursue an interest in access to justice issues through an LL.B. (1999) at UVic.

Jennifer Shepherd, Research Analyst, joined the Public Interest Advocacy Centre team in the fall of 2001. Prior to joining PIAC, Jennifer worked as a research analyst for the Consumers: Association of Canada conducting research in the areas of electronic commerce, service quality, and energy. This research included an analysis of third-party verification systems for electronic commerce and the importance of such systems to Canadian consumers. Jennifer authored the reports: *Analysing the feasibility of creating*

an electronic commerce site certification program (2001) and *ISO 9000 for the year 2000: Setting a standard for service delivery in business-to-consumer transactions* (2000). Jennifer graduated from the University of Guelph with a Bachelor of Applied Science, majoring in Consumer Studies.

The Action Group (TAG Consulting) is an Ottawa-based consulting firm specializing in survey techniques, assessment, data analysis and research and writing services. To date most of their work has been in the areas of health, corrections, and organizational issues such as stress management, team building and employee motivation. TAG has worked with several governmental and non-governmental agencies such as Correctional Services Canada, the Department of Justice, the Department of National Defence and the Canadian Public Health Association and have conducted several national studies, including the co-development, administration and analysis of a questionnaire examining quality of life in the Canadian Forces.

The principals are two Carleton University graduates: **Mr. Craig Dowden, Ph.D**. Candidate, who has published extensively in the area of corrections; and, **Mr. Neil Chambers, Ph.D.**, a personality psychologist with several articles on the importance of goal pursuit in health and well-being. TAG is affiliated both with Carleton University where Mr. Chambers is completing post-doctoral research and serves as the Associate Director of the Social Ecology Research Laboratory and with Harvard University's Dr. Brian Little, who provides expertise in the latest survey and assessment methodologies.

2. **Project management and policy guidance**

Jenny Hillard, VP Policy & Issues, CAC

Friederike Knabe, Project Manager, CAC

Jean Jones, Chair of CAC's Health Committee

James Savary, advisor on privacy issues, Volunteer Advisory Committee