

# **Briefing Note:**

## **eHealth, Bill 24 and Individual Consent**

May 20, 2008

Presented to the Hon. George Abbot, Minister of Health, by Representatives of

BC Civil Liberties Association  
BC Coalition of People with Disabilities  
BC Persons With AIDS Society  
Freedom of Information and Privacy Association

eHealth is proceeding rapidly with only grossly inadequate protections for (1) patient records confidentiality and (2) individuals' right to control their personal health information

- The Supreme Court has determined such protections are essential and such rights inviolable (please refer to Appendix C)
- Many British Columbians risk serious harm should their personal health information fall into the wrong hands – *including* those of various health care system personnel

eHealth is scheduled to “go live” in late 2008 with provincial laboratories and the Northern Health Authority, with “PharmaNet 2” (eDrug) scheduled to follow shortly thereafter

- None of the “legacy” systems involved is able to meet even the inadequate standards of records confidentiality and individual control of personal health information set out in Bill 24
- Leakage – unauthorized disclosure – is inevitable and, in some instances, will be more harmful in Northern Health than it would be elsewhere

The planned Integrated Case Management system being advanced and coordinated by the Office of the Chief Information Officer heightens the concerns with eHealth (and is an enormous problem on its own)

Bill 24, while proceeding in the right direction – and as moderately strengthened by the Government's proposed amendments – provides neither sufficient privacy protections nor sufficient scope for individuals to exercise effective control over their personal health information (please refer to appendices A and B)

Experience in other jurisdictions (United Kingdom, Germany, Australia, Manitoba, etc.) demonstrates that, if systems of electronic health records are not “got right” from the start, serious adverse consequences result

- Negative political consequences (leaks of personal health information, embarrassing system gaps and/or failures; dramatic budget overruns, especially for retroactive “fixes”)
- Widespread citizen and professional opposition, both passive and active (which, among other things, tends to make analyses of data collected unreliable)

Regardless, a massive public information campaign will be required to inform the citizenry of the advent of eHealth, and of their rights to control their personal health information

## Appendix A

### Bill 24 – problems and proposals at a glance

- Sections 4, 5, 14 and 15:
  - Clear distinctions must be drawn in Section 4 between nominal and aggregated access to personal health information; nominal access is acceptable for the purposes of clauses (a) through (e) and (i), but aggregated data only should be accessible via clauses (f), (g) and (h)
  - These concerns are exacerbated by the absence of this distinction in sections 5(b), 14, and 15
  - These concerns should be further addressed, as well, by giving every individual the option of placing a “do not contact for research purposes” order in their disclosure directives
- Section 8:
  - Section 8(2)(a) (as amended) will leave “types” of personal health information undefined – this is troubling; the term should be defined
- Section 9:
  - Section 9(1) and (2) only envisage individuals making and revoking disclosure directives; provision should be made to allow individuals to amend them, too
- Section 18:
  - Section 18(2)(a)’s reference to FOIPPA’s Section 33.1(e) remains even though the Government’s proposed amendments would delete Section 18(1)(a)’s reference to FOIPPA’s Section 33.2(c) – which is essentially the same thing; both elements should be deleted as they are needlessly broad and fly in the face of the Supreme Court’s determinations
  - Section 18(2)(a)’s reference to FOIPPA’s 33.1(p) permits access to nominal personal health information from foreign locations; the inherent dangers are obvious and this element should be deleted
- Sections 19 and 26
  - Section 19(1)(c)’s and 26(2)(h)’s provision of “bulk or regular” access to personal health information authorized by information-sharing agreements is excessively broad; especially given Section 18, “bulk or regular” access should be restricted to aggregated information only – either that, or individuals should be given the option to place a prohibition on the inclusion of their personal health information for such “bulk or regular” access purposes in their disclosure directives
- Section 26
  - Section 26(2)(c)’s granting to the Lieutenant Governor in Council the right to make regulations “limiting or prohibiting classes of persons from making disclosure directives” is excessive and without apparent need; if some classes of persons (e.g., minors caring for themselves) are to be excluded – and why would they be? – that should be provided in text of the Bill
- Other
  - Citizens without a personal physician should have the same protections available for their equivalent Electronic Medical Record information

## Appendix B

### Bill 24 – in-depth analysis

# Notes on Bill 24, the E-Health Act

BC Civil Liberties Association  
BC Coalition of People with  
Disabilities  
BC Freedom of Information and  
Privacy Association  
BC Persons with AIDS Society

#### BACKGROUND INFORMATION

Canadians have both a constitutional and a common law right to the privacy of their personal health information (PHI).

The Supreme Court has stated:

In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a *biographical core of personal information* which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.<sup>1</sup>

The essence of health privacy rights is, and traditionally has been, your right to control access to yourself and information about yourself. In practical terms, it has meant your right to give or withhold consent to the collection, use and disclosure of your information. Confidentiality and the requirement to obtain informed consent for the disclosure of personal information are the backbone of the health care system.

Citizens demand that their privacy be protected, which means that personal health information will be disclosed only to parties we approve, and that the information will be secure when it is disclosed. If there is a lack of confidence in privacy and security, the health care system starts to unravel.

#### Bill 24: Our concerns in a nutshell

Patient and privacy advocacy groups consulted with Ministry of Health officials for 1½ years on e-health Privacy and Security, and we were expecting to see privacy rights enshrined in the eHealth bill, as a guiding principle. We were greatly disappointed.

A pure 'consent model' for the collection, use and disclosure of personal health information (PHI) was rejected as unworkable. Because of this, the e-Health Act was predicated on the recognition that people in BC had the right to protect the privacy of their medical records

---

<sup>1</sup> *R. v. Plant*, [1993] S.C.J. No. 97 (Q.L.), para. 19 [hereinafter *Plant*].



through “disclosure directives” that allow individuals to limit access to all or part of their records by specific individuals or organizations or for specific purposes.


As it appeared at first reading, the E-Health Act does not include a true right of the individual to control the access, use and disclosure of one’s own personal information. This is because the means of control – “disclosure directives” – were completely at the discretion of the Minister and Cabinet. Amendments that are currently proposed mitigate this concern to some extent, but a person’s right to impose a disclosure directive is still very weak.




Secondly, Bill 24 will allow innumerable people who are not directly involved with individuals’ health care to have access to personal health information, without the affected individual’s informed consent – including officials such as planners, managers, and researchers. Access to personalized information is not necessary for these purposes.

This bill creates a huge conflict between on the one hand, the desire and legal right of individuals to keep their health information private and to control who has access to their health information, and on the other hand, the desire of government planners and managers for access to personal health information for a wide range of secondary purposes.


| <input checked="" type="checkbox"/> = At least some positive movement expected on this section |   | <input checked="" type="checkbox"/> = No movement apparent on this section  |
|--|---|---|
| BILL   | PROBLEM IN BILL 24  | CHANGES REQUIRED / EXPECTED   |
| s. 8<br>s. 9<br>s. 10<br><br><input checked="" type="checkbox"/>                               | <p><b>DISCLOSURE DIRECTIVES ARE INADEQUATE</b></p> <p><b>Disclosure directives</b> are supposed to allow individuals to limit access to all or part of their records by specific individuals or organizations, or for specific purposes.</p> <p>Unfortunately, Bill 24 gives near-total discretion over disclosure directives to the Minister, Data Stewardship Committees and Cabinet. This vitiates the intent of disclosure directives and reduces the right of privacy to the status of a privilege granted by government, revocable at will.</p> <p>(It is accepted that under special circumstances, such as individual medical or public health emergencies, access <i>might</i> be extended to non-named individuals, for limited times and purposes.)</p> <p><b>Regulations</b> – In addition to all the powers enjoyed by the Minister and Data Stewardship Committees to circumscribe disclosures, Cabinet by regulation can “limit or prohibit classes of persons from making disclosure directives“.</p> | <p>Bill 24 must contain an explicit right of citizens to impose disclosure directives concerning the collection, use and disclosure of their personal health information (PHI). This right should not be subject to the will of the Minister, Data Stewardship Committees or the L-G in Council, as it is presently – even with the amendments that have been proposed.</p> <p>Under the amendments expected to section 8, “Authorization of disclosure directives”, the bill should not under 8 (2)(a), (b) and (c), allow the minister to limit disclosure directives in the ways provided.</p> |


|   |   |   |
|---|---|---|
|   |   | <p>Section 9 (2)(b) should be removed or amended as a consequence</p> <p><b>Regulations – We note with approval that the removal of Section 26(2)(e) has been accepted. Section 26(2)(c) should also be removed.</b></p>  |
| <p><b>s. 3</b></p> <p></p>   | <p><b>BILL 24 s. 3 ALLOWS PARTS OF THE E-HEALTH SYSTEM TO BE LAUNCHED BEFORE DISCLOSURE DIRECTIVES ARE FULLY IMPLEMENTED</b></p> <p>The government intends to launch parts of the e-health system before the system of directives is functional. This is because making all the proposed data bases and systems capable of implementing disclosure directives and other requirements of the E-Health Act is a massive and very expensive undertaking. Some may not be ready for years!</p> <p>The bill allows the EHR system to be launched without adequate privacy safeguards. Because of this, the security dimensions are a potential nightmare.</p> <p>You're creating data bases and relations between data bases that didn't exist before and you are building multiple new avenues of access. There is no question that information will be lost, stolen and/or improperly disclosed. Once it is, it is out there permanently, beyond anyone's control.</p> | <p>No part of the EHR system should be launched – which is to say, no database should be designated as a Health Information Bank (HIB), regardless of the findings of the Stewardship Committee – until it can comply with all the privacy protections and other requirements of the e-Health Act.</p>                  |
| <p><b>S. 4</b></p> <p></p> | <p><b>BILL 24 ALLOWS ACCESS TO PERSONAL HEALTH INFORMATION BY OFFICIALS WHERE IT IS INAPPROPRIATE AND UNNECESSARY</b></p> <p>Bill 24 allows government officials to collect and use personal health information for a wide range of purposes for which it is not necessary.</p> <p>Access to PHI should be restricted within public bodies to those officials and functions directly involved with administration and delivery. Bill 24 allows officials to collect and use PHI for purposes of health services planning, management, development, maintenance and improvement.</p>   | <p>Section 4 should make a clear distinction between the various purposes for which PHI may be collected and used. Access should be restricted to the purposes for which it is strictly necessary.</p> <p>The different purposes should be separated out and clarified. Purposes should be categorized (and further</p> |



|  |  |  |
|--|--|--|
|  | <p>Managers only need <b>aggregate information</b>, not personal information, for these purposes. This is clearly laid out in <i>Information for Health: A Strategic Plan for Health Information Management in British Columbia</i> (Health Chief Information Officer Council, 2001)</p> <p>Access to PHI in such cases violates a fundamental rule of privacy protection and opens the door to broad dissemination of PHI throughout public bodies.</p> <p>This is not only a privacy breach, but a security threat as well. The risk of security breaches increases for every point of access and every unnecessary use.</p> <p><b>Definitions</b></p> <p>In the bill’s definitions “planning and research purposes” can refer to a whole range of purposes in section 4 that are neither planning nor research. Many are management purposes for which access to personally-identified information is not necessary at all.</p> | <p>defined) in five categories as follow:</p> <ol style="list-style-type: none"> <li>1. Health services planning, development, maintenance and improvement</li> <li>2. Health insurance and health service billing and administration</li> <li>3. Management, monitoring and evaluation necessary for the direct delivery of health care services (Primary uses of PHI for health care delivery)</li> <li>4. Public health surveillance and management</li> <li>5. Health research</li> </ol> <p>PHI should NOT be available for category 1.</p> <p>PHI should be available for purposes 2 through 4, but the users and types of information should be restricted to those strictly necessary for the purposes.</p> <p>PHI should be available for category 5, Health research, only with the consent of the patient or subject as previously granted in a disclosure directive.</p> |
| <p>s. 5</p> <p></p> | <p><b>DISCLOSURE OF HEALTH INFORMATION IS ALSO ALLOWED WHERE INAPPROPRIATE AND UNNECESSARY</b></p> <p>See above – “planning and research purposes” include purposes in section 4 (g) that are neither planning nor research. These include health services, maintenance, improvement, development, management, monitoring and evaluation.</p> <p>5 (b) is unclear on whether a disclosure for “a planning or a research purpose” could be made <b>outside Canada</b>.</p>  | <p>The nature of the various purposes must be clarified to ensure that access to PHI is actually necessary and appropriate for each activity.</p> <p>5 (b) must be clarified to ensure that disclosure for “a planning or a research purpose” cannot be made outside Canada.</p>   |

|   |   |   |
|---|---|---|
| <p>s. 14</p> <p></p>   | <p><b>DISCLOSURE FOR PLANNING OR RESEARCH PURPOSES SHOULD BE NARROWED</b></p> <p>Once again, access to PHI should be allowed only where it is necessary to achieve the stated purpose. This is a primary principle of privacy protection. S. 14 omits this 'necessity' principle.</p> <p>And again, we see the problem of the conflation of "planning and research purposes". There is no justification for dealing with very diverse purposes in such a broad way. (See above.)</p>  | <p><b>New proposal</b></p> <p>S. 14 (2)(a) should be amended to add the word 'necessary' so that it reads that a request for disclosure of PHI may be approved where "(a) the request is <b>necessary</b> for a planning or research purpose.</p>   |
| <p>s. 15</p> <p></p>   | <p><b>DISCLOSURE OF PHI FOR HEALTH RESEARCH PURPOSES IS ALLOWED WITHOUT INFORMED CONSENT</b></p> <p>We strongly object to the idea that individuals' health information should be available for research purposes without informed consent.</p> <p>As one example, more than just a few HIV-positive British Columbians would be horrified to be contacted out of the blue by some researcher or other purporting to do research on this or that aspect of HIV; the psychological and emotional effects could be severe, especially in smaller centres.</p> | <p>At the very least, individuals should be permitted to create a disclosure directive requiring that their PHI not be used for research purposes. This could take the form of a "do not contact for research purposes" tick box or some such in the standard disclosure directive.</p> <p>Studies suggest that very few people would be interested in doing so.</p> <p>Studies also indicate that a majority of people feel they should have a right of consent for research uses of their PHI</p> |
| <p>s. 17</p> <p></p> | <p><b>A KEY PRINCIPLE OF BILL 24 – AND A KEY SELLING POINT OF E-HEALTH – IS THAT INDIVIDUALS WILL HAVE ELECTRONIC ACCESS TO THEIR OWN PERSONAL INFORMATION. HOWEVER, SOME PHASES OF THE E-HEALTH SYSTEM ARE SCHEDULED FOR LAUNCH WELL BEFORE THIS CAPABILITY EXISTS</b></p> <p>Section 17 provides for individuals to have access to</p>  | <p>As noted above with regard</p>   |

|   |  |  |
|---|--|--|
|   | <p>their own eHealth records. Very good.</p> <p>Unfortunately, current plans call for the first phase of e-Health (the Provincial Laboratory Information Systems “domain”) to go “live” in the Northern Health Authority in the middle of November – and it is not now scheduled to be able to allow individuals to view their lab records on-line.</p>  | <p>to Section 3, no component of the e-Health system should go online until disclosure directives and all other privacy protections are up and running.</p>  |
| <p>s. 18</p> <p><input checked="" type="checkbox"/></p> | <p><b>“PURPOSES FOR WHICH DISCLOSURE IS ALWAYS ALLOWED” ARE FAR TOO BROAD AND UNDEFINED IN SECTIONS 18(1)(a) and 18(2)(a)</b></p> <p>After limiting disclosures of personal information to fairly narrow, health-related purposes in section 5, Bill 24 then throws out all those limitations in section 18, by allowing disclosures as set out in sections 33.2 (c) and 33.1 (1)(e) of the <i>Freedom of Information and Protection of Privacy Act</i> (FOIPPA).</p> <p>These sections allow disclosure of PHI to almost any government official of any ministry – including government ministers – and for any number of undefined purposes.</p> <p>This is in conflict with the general intent of Bill 24 which is to limit disclosure to health care officials and purposes. It opens the door wide to unlimited disclosures and therefore renders any restrictions in the bill useless.</p> <p>If that is what was intended, Bill 24 may as well not exist. We may as well just leave the management of personal health information to the FOI act.</p> <p>FOIPPA s. 33.2 (c) states</p> <p><b>33.2</b> A public body may disclose personal information referred to in section 33 inside Canada as follows:</p> <p>(c) to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of the officer, employee or minister;</p> <p>FOIPPA s. 33.1 (1) states</p> <p><b>33.1 (1)</b> A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:</p> <p>(e) to an individual who is a minister, an officer of the public body or an employee of the public body</p> | <p>We note with approval that Section 18 (1)(a) is expected to be amended to delete the reference to FOIPPA section 33.2 (c).</p> <p>Section 18 (2)(a) should also be amended to delete the reference to FOIPPA section 33.1 (1)(e).</p> |

|   |   |  |
|---|---|--|
|   | <p>other than a service provider, if</p> <ul style="list-style-type: none"> <li>(i) the information is necessary for the performance of the duties of the minister, officer, or employee, and</li> <li>(ii) in relation to disclosure outside Canada, the outside disclosure is necessary because the individual is temporarily travelling outside Canada</li> </ul>  |  |
| <p>s. 18</p> <p></p> | <p><b>BILL 24 ALLOWS PERSONAL HEALTH INFORMATION TO LEAVE CANADA FOR DUBIOUS PURPOSES</b></p> <p>Section 18 (2)(a) allows an administrator to disclose PHI <b>inside or outside Canada</b> for “a purpose described in section 33.1 (1)(p) of the <i>Freedom of Information and Protection of Privacy Act</i>”, which states:</p> <p><b>33.1</b> (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:</p> <p>...(p) the disclosure</p> <ul style="list-style-type: none"> <li>(i) is necessary for             <ul style="list-style-type: none"> <li>(A) installing, implementing, maintaining, repairing, trouble shooting or upgrading an electronic system or equipment that includes an electronic system, or</li> <li>(B) data recovery that is being undertaken following failure of an electronic system</li> </ul>             that is used in Canada by the public body or by a service provider for the purposes of providing services to a public body, and           </li> <li>(ii) in the case of disclosure outside Canada,             <ul style="list-style-type: none"> <li>(A) is limited to temporary access and storage for the minimum time necessary for that purpose, and</li> <li>(B) in relation to data recovery under subparagraph (i) (B), is limited to access and storage only after the system failure has occurred.</li> </ul> </li> </ul> <p>This may appear to be a limited exception, but we are assured by IT professionals that routine industry practices would allow data to remain outside Canada for significant periods for the purposes described – certainly long enough to allow access under legislation such as the <i>USA PATRIOT ACT</i>.</p> | <p>Given the sensitivity of the information at issue, there should be an absolute ban on access to this information from outside Canada without the express consent of the patient</p> |

|   |  |  |
|---|--|--|
|   | <p>It is well known that personal information that leaves our borders does not enjoy the legal protections it does in Canada. For example, such information may be accessed under the <i>USA PATRIOT ACT</i> without our knowledge.</p> <p>There are some circumstances in which it is almost impossible to prevent data from leaving Canada, but there are very few valid reasons to allow the personal information we place in the trust of government bodies to cross borders.</p> <p>Specifically, this should not be allowed for the installation or maintenance of the electronic data bases covered by Bill 24. The kinds of PHI involved are the most sensitive that exist – and also the most valuable to commercial entities, security agencies and cyber-criminals.</p>   |  |
| <p>s. 19</p> <p></p> | <p><b>BILL 24 ALLOWS BULK DISCLOSURES OF PERSONAL HEALTH INFORMATION IN UNDEFINED AND EXTREMELY BROAD CIRCUMSTANCES</b></p> <p>Section 19(1)(c) makes reference to what would amount to routine disclosure “if personal health information is to be disclosed on a bulk or regular basis.”</p> <p>To allow sharing of PHI to "any agency or ministry of the government of BC, of another province or of Canada, including Crown corporations and "a prescribed body that is public in nature" is very unusual and unacceptable in an act that is supposed to protect privacy</p> <p>Disclosures on a "bulk or regular" basis are clearly envisioned and yet, not defined. It is difficult to conceive of the "bulk and regular" provisions of PHI that could ever be justified without the informed consent of the individuals concerned.</p> <p>Sec.26(2)(h) [(g) as amended] specifies that the Cabinet is to define what this phrase means by regulation. This is yet another potentially enormous hole in privacy protection that is left to the whim of the Government.</p> | <p>Sections 19(1)(c) and the consequent 26(2)(h) [(g) as amended] are entirely too broad and ill-defined. Ideally, both should be deleted. Failing that, clear detailing of precisely what PHI is to be disclosed to precisely which person or body on precisely what bulk or regular basis should be set out in the Act itself. That way citizens may at least know what the risks are.</p> |

|  |   |   |
|--|---|---|
| <p>s. 26</p> <p></p>              | <p><b>Bill 24 PERMITS THE L-G-IN-COUNCIL TO “LIMIT” OR “PROHIBIT” ENTIRE “CLASSES OF PERSONS” FROM MAKING DISCLOSURE DIRECTIVES</b></p> <p>In discussions with Ministry personnel, it was suggested that Section 26(2)(c) was entered in the Bill to enable the addressing of peculiar circumstances – such as occur when persons not yet 18 years of age are, nonetheless, in situations where they are living on their own or with non-guardian friends and are responsible for themselves.</p> <p>Setting aside the question of what good is be had or done by depriving such persons of the benefits of disclosure directives, it must be said that including so broad and ill-defined an authority for the Government to frustrate individuals’ right to determine the disposition of their own personal health information would seem to be one of those rare instances worthy of the term “Draconian”.</p> | <p>Section 26(s)(c) should be deleted.</p> <p>Any instance where a given “class” of persons is to be deprived of the use of disclosure directives should be spelled out in the Act – assuming there is any legitimate instance to be had.</p>   |
| <p><b>New Issue</b></p> <p></p> | <p><b>BILL 24 FAILS TO PROTECT DOCTOR-PATIENT CONFIDENTIALITY FOR PEOPLE SERVED BY COMMUNITY CLINICS</b></p> <p>A patient’s medical record held by a physician (the Electronic Medical Record, or EMR) is protected for those fortunate enough to have a personal physician because that medical record will remain separated from the EHR.</p> <p>This protection does not extend to the huge numbers of people who receive their primary medical care through community clinics or who receive services through street services, youth clinics, STI clinics, and so on. In these cases, the records which otherwise would be considered to be EMR’s will flow directly into the EHR.</p>  | <p><b>New proposal</b></p> <p>At the first opportunity, Bill 24 should be amended to provide equal confidentiality and privacy protection of a personal medical record for those who lack a personal physician because of social disadvantage or the unavailability of family practitioners.</p> <p>We suggest that the College of Physicians and Surgeons and the BCMA should create a protocol for protecting these patient records in a way similar to how physicians’ Electronic Medical Records will be protected.</p> |

## *Appendix C*

### Pertinent Supreme Court Determinations

...it has long been recognized that this freedom not to be compelled to share our confidences with others is the very hallmark of a free and democratic society.<sup>2</sup>

In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a *biographical core of personal information* which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.<sup>3</sup>

[t]he values protected by privacy rights will be most directly at stake where the confidential information contained in a record concerns aspects of one's individual identity or where the maintenance of confidentiality is crucial to a therapeutic, or other trust-like, relationship.<sup>4</sup>

---

<sup>2</sup> *R. v. Mills* (2000), 180 D.L.R. 1 at 46

<sup>3</sup> *R. v. Plant*, [1993] S.C.J. No. 97 (Q.L.), para. 19

<sup>4</sup> *R. v. Mills*

## *Appendix D*

### Declaration of Medical Privacy Rights

(as Prepared by the Freedom of Information and Privacy Association)

The Right to Privacy is a human right and is fundamental to my dignity as a human being.

My right to privacy extends to all my personal health information, regardless of the format in which it is recorded. Any personal health record maintained on me by any health care provider is created through a special relationship, with the expectation that my information will remain confidential. The confidential nature of this relationship exists to safeguard and promote my physical and mental health. Any violation of this confidential relationship may adversely affect my health and is a violation of my right to privacy.

The right to privacy affirms my right to control access to and use of my personal health information. Any access or use without my consent is a violation of my right to privacy.

Fundamental to my right to privacy of health information is the right to:

- a) be told why specific information is requested and if it will be part of a physical record,
- b) know who will have access to any of my health information and for what purpose,
- c) refuse access to all or portions of my information,
- d) expect an audit trail that will identify who has accessed my health information,
- e) expect my health information will be maintained in a secure environment that will prevent any unauthorized access,
- f) request and receive an accurate and complete copy of my health records in a timely fashion,
- g) have corrected any factual error in the records. If there is a disagreement about the accuracy of the records, it is my right to have the disputed information clearly identified and to append to the records what I believe to be the correct information,
- h) expect the information will be retained for a length of time appropriate only to the primary reason for which it was obtained. Any retention beyond this length of time must be done with my consent, and
- i) seek an effective remedy should any of these rights be violated.

## *Appendix E*

### Organizations represented

#### **BC Civil Liberties Association**

The B.C. Civil Liberties Association was established in 1962 and is the oldest and most active civil liberties group in Canada. The organization is formed by a group of citizens who volunteer their energy and talents to fulfill the organization's mandate: to preserve, defend, maintain and extend civil liberties and human rights in British Columbia and across Canada. The BCCLA is an autonomous, non-partisan charitable society.

Represented by: Micheal Vonn, Policy Director

#### **BC Coalition of People with Disabilities**

The BC Coalition of People with Disabilities is a provincial, cross-disability advocacy organization. Its mandate is to raise public and political awareness of issues that concern people with disabilities. The organization hopes, through its work, to facilitate the full participation of people with disabilities in all aspects of society and to promote independence.

Represented by: Jane Dyson, Co-Director, Advocacy Access

#### **BC Persons With AIDS Society (BCPWA)**

BCPWA Society is dedicated to empowering persons living with HIV disease and AIDS through mutual support and collective action. It is Western Canada's largest AIDS organization with a membership of more than 4,400 HIV-positive individuals. Unique among major HIV/AIDS agencies in Canada, BCPWA Society's Board of Directors is composed entirely of HIV-positive members. The Society provides support and advocacy services, treatment information and volunteer opportunities for its many diverse members.

Represented by: Glyn Townson, Chairperson  
Ross Harvey, Executive Director

#### **Freedom of Information and Privacy Association (FIPA)**

FIPA is a non-partisan, non-profit society that was established in 1991 to promote and defend freedom of information and privacy rights in Canada. Its goal is to empower citizens by increasing their access to information and their control over their own personal information. They serve a wide variety of individuals and organizations through programs of public education, public assistance, research, and law reform.

Represented by: Darrell Evans, Executive Director