

# Consumers' Association of Canada (Alberta)

[www.albertaconsomers.org](http://www.albertaconsomers.org)

(780) 426-3270

## Submission to the Standing Policy Committee on Health, Alberta Legislature

Re: **Bill 52, Amendments to the Alberta Health Information Act**

*(Speaking Notes for Presentation by Wendy Armstrong Feb. 4<sup>th</sup>, 2009)*

***“Technology switches the opportunities for subversion from individuals to organizations.”***

Mark Lisac, Edmonton Journal, 1995

Appendix 1 – The use of databases to segment banking customers

Appendix 2 - Additional Information on Manitoba Health Policy Centre

Appendix 3 – Additional Information on frequency of data breaches

Appendix 4 – Verification Inc. pre-employment form

Appendix 5 – Authorization for RBC application for insurance

### Recommended Reading

Who's got and who wants your medical information? See News and Updates at Alberta Consumers' Association [www.albertaconsomers.org](http://www.albertaconsomers.org)

National Identity Cards: Biometrics and the Consumer: Displacing the Personal from the Person The Public Interest Advocacy Centre (Ottawa), 2007, [www.piac.ca/privacy/](http://www.piac.ca/privacy/)

Silversides, A., Merchant Scientists: How commercialization is changing research in Canada The Walrus Magazine, May 2008, <http://www.walrusmagazine.com/articles/2008.05-science-and-commercialization-ann-silversides/>

Jane Elliott: Blue-Eyes/Brown-Eyes Exercise

<http://www.janeelliott.com/>

<http://www.pbs.org/wgbh/pages/frontline/shows/divided/>

**Recommended Viewing:** <http://www.aclu.org/pizza/images/screen.swf>

The American Civil Liberties Union takes a break from its serious side to illustrate new technologies and the blurring of government, health and commercial information.

<http://www.aclu.org/privacy/gen/15737prs20040726.html>

## **A “Real World” Reality Check**

Given the limited lead-time, we have not prepared a brief, however, some of our past submissions related to expanding uses of health information and HIA and PIPA can be found on our website at [www.albertaconsurers.org](http://www.albertaconsurers.org) (See under *News and Updates*.) I have also provided a handout with some examples of application forms I will refer to in my presentation.

*See Appendices.*

The most important message we would like to give to you today is that “good intentions” do not obviate the need for protection of citizens from deliberate or inadvertent harm – and that “good intentions” can sometimes be misguided or misinformed.

. . . And that people are not just “patients”. Our lives and relationships outside the health care system also have a powerful influence on our health and wellbeing.

In my presentation, I will briefly touch on four points:

- Putting the cart before the horse
- How the loss of medical confidentiality affects physical and mental health
- The larger social and health care context
- Lessons learned in other realms

I would also like to touch on what we think is *a better way* to go with public interest research using health information databases.

## **1. Putting the cart before the horse.**

In our view, current HIA amendments put “the cart before the horse” by asking the public and MLAs to make decisions with no practical knowledge of current or future applications of health information registries and electronic health records and the rules governing them - e.g., Netcare, E-clinician, physician records.

Many promises made regarding safeguards have been repeatedly broken since the HIA was first enacted – and more are being removed in this Bill. In particular, removal of the requirement for patient consent in 2003 means that most Albertans have no idea of the scope of their personal information in Netcare and how it is accessed and used without their knowledge.

Therefore we strongly encourage you to not proceed with this Bill, but instead begin a meaningful dialogue with the public.

***We believe Albertans have “a right to know” in order to protect their own interests and influence public policies.***

The problem is that while proponents like to talk about the benefits of electronic records, similar to the situation with adverse drug reactions and adverse surgical events, the adverse effects of electronic health records and databases are rarely tracked or reported.

***It is also important to remember; the problem is not the existence of electronic records, but the design and rules.***

Today we would like to fill in some of the blanks for you as to why many of the amendments are so problematic.

## **2. How the loss of medical confidentiality can affect mental and physical health**

Many amendments – e.g. undefined health information repositories, mandatory disclosure, the seeming inability of system operators to effectively mask sensitive information, the inclusion of many more entities within the circle of information sharing and plans to upload more detailed clinical records to Netcare - appear to spell the end of any notion of medical confidentiality. It will also reduce public transparency.

A widespread public fear is that of being socially or medically labeled or stereotyped in a way which leads to bias and prejudice and the loss of benefits – such as a job, a loan, insurance, renting an apartment or access to unbiased medical care and the good will of health professionals.

Medical labels are often transient, subject to bias and easily misinterpreted.<sup>1</sup> Just see how you are treated with a label of “mild dementia” – “depression” – or even “diabetic”, let alone a label of HIV.

Stigma can have a powerful influence on sense of self worth and response to others. This is demonstrated in Jane Elliott’s now famous Blue-Eyes/Brown-Eyes Exercise which labels participants as inferior or superior based solely upon the color of their eyes and exposes them to the experience of being stigmatized as a minority.<sup>2</sup>

When people feel threatened, it increases the stress they experience. There is now a fair body of evidence suggesting that chronic social stress can lead to continuous output of cortisol, which in turn can negatively influence physical health.<sup>3</sup>

Those who feel threatened are also less likely to trust, cooperate or deal in good faith.

A 1993 survey by the Canadian Medical Association found that 7% of Canadians had not sought out diagnosis or treatment because of worries about how it might affect other aspects of their lives such as insurability or employment. **By 1999, 11% held back information from a health provider because they were concerned about who it would be shared with or what purposes it would be used for.**

Failing to seek treatment or disclose relevant information limits the ability of a doctor to accurately and effectively diagnose and treat. It also puts the public at risk from contagious diseases.

Research by Gary Marx has shown that public resistance to information surveillance occurs in many invisible ways, including individuals obscuring their identities, distorting their data, refusing to comply and so on.<sup>4</sup> Efforts of Canadians to protect themselves from lost benefits leads to less reliable data for researchers as well as increased personal and public health risks.

### **3. The larger social and health care context**

Companies now track and sell information about most of the transactions in our daily lives, facilitated by the decreasing costs of data processing and the increased use of “virtual” money (debit, credit), loyalty cards and the Internet, all which leave a digital footprint.<sup>5</sup> This information reveals much

---

<sup>1</sup> Caplan and Cosgrove, Bias in Psychiatric Diagnosis, 2004 and Dr. Jerome Groopman, How Doctors Think, 2007.

<sup>2</sup> Ironically, stigmatizing individuals is now a common form and/or outcome of many health promotion activities.

<sup>3</sup> CBC Ideas Program Podcast, Sick People or Sick Society, Part 1, 2008  
[http://podcast.cbc.ca/mp3/ideas\\_20080303\\_4892.mp3](http://podcast.cbc.ca/mp3/ideas_20080303_4892.mp3)

<sup>4</sup> See related articles on website <http://web.mit.edu/gtmarx/www/garyhome.html>

<sup>5</sup> On the Data Trail: How Detailed Information About You Gets Into The Hands Of Organizations With Whom You Have No Relationship, Publications, CIPPIC, 2006,  
<http://www.cippic.ca/documents/May1-06/DatabrokerReport.pdf>

about our likes and dislikes, movements, status, means and actions. The chair of the Democratic Party in the U.S. has recently been quoted saying, "We can predict voter preference more reliably from credit-card data than from voter registration [party affiliation] data."

Originally intended for retail marketing purposes, use of this collected information has now expanded to other relationships in our lives – e.g., employers, landlords, the police, insurers and bankers - a phenomenon called **function creep**: information collected for one purpose is then used for other purposes.

There is increasing overlap, sharing and merging of public and private sector databases.

### ***The Catch 22: External Authorizations***

The Catch 22 of having the right to access your own information is that companies, organizations and agencies can *require* you to authorize their access to your information held by other third parties as a condition for a job, service or other benefit, including electronic medical records. Denying access is interpreted as having something to hide.

Nowadays, few people give a second thought to signing authorizations to allow a company or agency to access their "confidential" information as part of an application for work or insurance.<sup>6</sup> Nor do they have any real choice.

I've included two examples of forms people are often asked to sign; one for a remarkably extensive pre-employment background check by Verification Inc. and another for an RBC health or disability insurance policy.

*See Appendix 4 and 5.*

Despite having been invited to apply for the job based on past work with the company, the refusal of a recently hired office worker in Edmonton to sign the attached Verification Inc. form (Appendix 4) out of concern about the extent of information requested, the potential for identity theft and the lack of available information about Verification Inc. led to immediate dismissal.

Also, few people have any idea of the extent or accuracy of information held by third parties – or within the health care system.

For example, when a young woman starting her own business in Ontario applied for a disability insurance policy she was surprised to be turned down because the company said her medical records showed that she had a history of repeat physician visits for "psychological counseling". It turned out her physician, someone her family had gone to for years, had been billing all these appointments as psychological counseling because she spent so much time talking when they went in with routine problems. When the woman

---

<sup>6</sup> Due to the increasing costs of employer-sponsored benefit plans as a consequence of cost shifting from public Medicare programs to private payers, companies are far more interested in the health of job applicants – and their families – than they were in the past.

confronted the doctor, the physician said, "Well how else am I going to get paid for the real amount of time I spend to provide you with good care?" The irony is that this visit was also billed as psychological counseling. No disability insurer will touch this young woman because all such information is shared in an industry-run database.<sup>7</sup> Nor does she feel she can destroy her parents' relationship with the doctor by filing a complaint.

### ***Databases used to sort, segment and discriminate***

Electronic databases are now used in large dominant industries such as banking, telecommunications and energy to segment customers, reduce genuine competition and penalize customers with fewer resources. For an example of how this has affected banking services.

*See Appendix 1.*

Similarly, over the last decade, provincial and federal governments have adopted the use of large electronic databases to sort and label citizens in ways that can limit our life choices and chances. The loss of universality of social security benefits, including health benefits, requires more detailed information about income, family resources and other criteria to determine eligibility for benefits, opening the door to hidden bias.

Reasons cited by the Alberta government for development of an integrated electronic health information system during consultations in 1997 included shifting public expenditures for healthcare to auto insurance policies through new Third Party Liability legislation; determining co-payments and eligibility for access to publicly funded health care and facilitating contracting out and managed care models.<sup>8</sup>

### ***Commercial drivers for electronic health records and registries***

It's also important for you to know about the increasing commercialization and powerful influence of the pharmaceutical industry on health research and health care today -and how one of the drivers behind the creation of EHRs, disease registries and biobanks is to facilitate clinical trials of new drugs.<sup>9</sup>

Clinical drug trials are a growing business in Canada and more than 80% of these trials are funded by the pharmaceutical industry.<sup>10</sup> The number of Phase 1 trials (testing for safety in humans) approved by Health Canada in 7 days increased from 138 in 2001 to 630 in 2002 and 1006 in 2005.

---

<sup>7</sup> All information collected from the insurance applications (and claims) of over 500 companies is stored in a shared database (the MIB) located in Massachusetts.

<sup>8</sup> Reported in Integrated Health Information Systems: Background Discussion Paper, CAC (Alberta), 1997

<sup>9</sup> A roadmap to research uses of electronic health information, draft paper by Willison et al

<sup>10</sup> Money, Drugs and Ethics 2003 Michener- Deacon Fellowship

<http://www.michenerawards.ca/english/repmunro2003.htm>

Clinical Trials in Canada: Quality with Cost Advantage, Industry Canada, 2003 (not available online)

#### 4. Lessons Learned From Other Sectors

Protecting the integrity of databases holding personal information is not only costly, but difficult to assure.<sup>11</sup> Sloppy data entry, coding, confusion with common names/locations, bias or prejudice, breaches, unauthorized uses and fraud are common reasons for widespread inaccuracies in databases.

##### ***Identity Theft and Fraud***

The existence of electronic databases and ease of access to so much personal information at the touch of keystroke has been a major driver in the success of an international fraud industry dominated by **organized crime**.<sup>12</sup> Identity theft is the fastest growing crime in Canada with tens of thousands of consumers victimized each year.<sup>13</sup> It also leads to major inaccuracies in records, including criminal records.

Data breaches are common and widespread. In Canada, there is no requirement to notify to affected parties or authorities when a data breach occurs, whether that breach occurs through an outside assault, internal error or carelessness.

**We also now know that the first response to a problem isn't always the right response.** The first response by merchants and public agencies faced with the growth of identity theft and fraud is often to collect and store even more personal details in an electronic database in order to authenticate someone's identity. Ironically, this greater detail creates an even greater risk fraud and identity theft should a data breach occur, which they do with remarkably regularity.

We know that more contracting out, particularly to companies with multiple lines of business and subcontractors (or other jurisdictions), increases the number of data breaches, errors, and risk of identity theft and fraud.<sup>14</sup>

We know that anonymous data can often be re-identified through data matching - primarily for sub populations such as a group of professionals - rather than whole populations - unless exceptional safeguards are in place.

We know that the greater the size of a database, the greater the number of uses and the greater the number of users, the greater the problems and the less user-friendly applications are for different purposes.

---

<sup>11</sup> See National Identity Cards: Biometrics and the Consumer: Displacing the Personal from the Person, The Public Interest Advocacy Centre, 2007, [www.piac.ca/privacy/](http://www.piac.ca/privacy/)

<sup>12</sup> In 2006, 8000 victims reported losses of \$16 million to the Canadian Anti-fraud Call Centre. The Canadian Council of Better Business Bureaus estimates that identity theft may cost consumers, banks and credit card firms and other businesses more than \$2 billion annually.

<sup>13</sup> See section on Identity Theft on PIAC website at <http://www.piac.ca/privacy/>

<sup>14</sup> For example, see *Tackling ID Theft: Legal and Policy Approaches*, Presentation, P. Lawson, Canadian Internet Policy and Public Interest Clinic (CIPPIC), 2007, see page <http://www.cippic.ca/bulletin/>

*We don't know if and how much of our anonymized health data has been sold to insurance companies or drug companies here in Alberta, although we do know that most provincial governments have been approached about such sales.*

**In summary, we believe there is evidence for caution in moving ahead with this legislation or the future and value of any electronic health records will be put at risk. So will the health and safety of Albertans.**

#### **5. A better way to go with health information research repositories.**

Finally, I will touch briefly on the creation of health information research repositories identified in Bill 52. Although our organization has long championed the creation of a university-based arm's length health policy research centre in Alberta, our support for repositories is entirely predicated on the limited use of such databases by such a Centre and appropriate governance structures similar to those in Manitoba.

We would also like to see a commitment to research in the public interest and public disclosure of results as well as public involvement in governance.

*See Appendix 2.*

**In closing, the questions we would like to leave with you are:**

***Will the removal of important protections for consumers, workers, citizens and patients in the sharing of their medical information and the collection of ever more information in electronic databases truly solve our health care woes?***

***Or will it simply divert our attention from other solutions, compromise the safety and quality of care, increase our vulnerability to fraud and exploitation, and cost a great deal of public money?***

Thank you for your time and attention.

## Appendix 1: The Use of Databases for Market Segmentation <sup>1</sup>

As governments have retreated from their traditional role of protecting small consumers in inherently non-competitive industries, electronic databases have allowed companies, particularly dominant banking, telecommunication and energy companies, to segment their large customer base into high value customers and low value customers. High value customers obtain high quality service, special pricing benefits, and regular contact. Low value customers are shifted to telephone trees and call centre staff in India or Virginia with no authority to act.

In the early 1990s, as the financial services sector was being deregulated, banks reduced their hours and closed hundreds of branches. They also got out of the small loans business. High-end customers were shifted to high interest rate credit cards; low-end customers to new (and even higher cost) alternative credit and cheque cashing markets such as "pay-day" loan companies. The inability of many Canadians to access historic banking services and affordable small loans in this era of automatic deposits and bill payment is creating a major dividing line in Canada.<sup>2</sup>

The problem with this type of market discrimination is that it leads to completely different perceptions of the price and quality of services among the population. There is less pressure for companies to improve quality or prices across the board.

Jacques St. Amant with Options Consommateurs, points out the frustration of consumers who do not understand and cannot control or influence the decisions about accessing and using their money in this new era. "Decisions about you are made on the basis of your virtual twin [i.e. information in electronic databases] by a machine with which you cannot argue."

The price you see on your computer for an advertised product may also differ from that of your neighbour. In 2005, the Annenburg Public Policy Center released a study entitled, "*Open to Exploitation*," which found that most Americans have no idea that Internet merchants often charge different prices to different consumers for the same products. According to the study, nearly two-thirds of adult Internet users incorrectly believe it is illegal to charge different people different prices, a practice retailers call "price customization".

The major reason cited by banks for mergers is to take advantage of efficiency gains with shared databases for marketing and market segmentation purposes.<sup>3</sup> Reasons cited by the Alberta government for creation of an integrated health information system during consultations in 1997 included shifting costs for healthcare expenses to auto insurers through new third party liability legislation, determining individual co-payment and access to public services and facilitating contracting-out services.<sup>4</sup> There is no evidence that any efficiency gains from the use and linkage of electronic databases are passed on or fairly distributed to the public.

The banking industry and its shift to virtual money have also played a significant role in the growth of identity theft and fraud.

---

<sup>1</sup> Based on excerpt from draft paper, 2008, Armstrong W.

<sup>2</sup> Many landlords and utility and telephone companies refuse to take cash.

<sup>3</sup> See *Consumers Assess Mergers Among Big Banks*, CAC, 2003  
[http://www.consumer.ca/pdfs/bank\\_mergers.pdf](http://www.consumer.ca/pdfs/bank_mergers.pdf)

<sup>4</sup> *Integrated Health Information Systems: Background Discussion Paper*, CAC (Alberta), 1997

## **Appendix 2: Governance of Research Repositories**

**The Manitoba Centre for Health Policy (MCHP)** is a research unit in the Department of Community Health Sciences, Faculty of Medicine, and University of Manitoba. The Manitoba Centre for Health Policy through the University of Manitoba is the trustee for the Population Health Research Data Repository. Public bodies collect all data in this repository. Research using these data is permitted by privacy legislation if:

- It is for statistical or research purposes,
- It is in the public interest, and
- The results remain in the public domain

The Health Information Privacy Committee (HIPC) in Manitoba is also responsible for approving health research projects that use personal health information held by a government department or agency.”

Without explicit commitment to agreed “public good” purposes for research repositories in the HIA, our fear is that this Bill will serve as to be enabling legislation for governments and private partners to collect, commodify, and use detailed information about our personal lives for commercial purposes.

## Appendix 3: Data Breaches

Data breaches can be internal or external. Below are some examples of data breaches and some of the outcomes. Theft or tampering of personal information is often very hard to detect when many people have access to databases and there may be a significant lag time between the occurrence of a breach and detection. The theft will usually not be detected until the victim discovers unauthorized activity in accounts, is contacted by a financial institution or debt collectors or denied credit. Or, when a victim is refused social benefits (passport), employment, insurance or the information comes to light in a civil court case. Authorities are much more likely to believe information in a database than information provided by the victim.

*A random scan of media reports on any single day will find multiple stories of personal data being lost by or stolen from corporations and governments (see <http://ehip.blogs.com/ehip/> for an ongoing tally).*

**Following are some examples of stories in the last few years.**

**Bell Hit With Theft of Data on 3.4 Million Customers** Tuesday February 12, 2008 Bell Canada has disclosed that it recovered data on 3.4 million customers after the information was stolen four weeks ago. Montreal police have arrested one person. <http://www.cbc.ca/canada/story/2008/02/12/bell.html>

**Canadian Bar Association Hit By Security Breach** Thursday January 10, 2008 An audit of the Canadian Bar Association online web systems has revealed unauthorized third party access to the system during the recent holiday period. The CBA has advised affected members that "Your records may have been affected by this unauthorized activity."  
[http://www.cba.org/CBA/News/2008\\_Releases/2008-01-09\\_advisory.aspx](http://www.cba.org/CBA/News/2008_Releases/2008-01-09_advisory.aspx)

**Passport Canada Suffers Massive Privacy Breach** The Globe and Mail reports Passport Canada has suffered a massive privacy breach that resulted in online availability of applicant information. December 04, 2007

**Deloitte Survey of Companies** According to a study of financial institutions conducted by Deloitte between November 2005 and February 2006, 78 per cent of Canadian respondent companies said they had been subject to some kind of external security breach in the last 12 months. Neil Sutton, "Canadian financial institutions among global leaders in security", IT Business (13 June 2006), <http://www.itbusiness.ca/it/client/en/home/News.asp?id=39775&cid=7>.

**Identity theft feared after credit information stolen** *The Globe and Mail*, 16 March 2004), <http://www.e-commercelert.com/article624.shtml>

**Bank fraud trail leads to former outsourcing help**  
<http://www.itworldcanada.com/a/Security/3185acb5-1b95-4019-8bf9-a146ecf8446f.html>

**Trial by CCTV claims innocent victim: Mistaken identity**, Britain, April 2001  
[http://www.theregister.co.uk/2001/04/19/trial\\_by\\_cctv\\_claims\\_innocent/](http://www.theregister.co.uk/2001/04/19/trial_by_cctv_claims_innocent/)

**Your Rights Online: US Consumers Clueless About Online Tracking**  
<http://yro.slashdot.org/yro/07/11/05/2351248.shtml>

### **15,000 want off the U.S. terror watch list**

[http://www.usatoday.com/news/washington/2007-11-06-watchlist\\_N.htm](http://www.usatoday.com/news/washington/2007-11-06-watchlist_N.htm)

**UK: ' I was falsely branded a paedophile'** With ID fraud on the rise, the assumption is you'll lose money which can be claimed back. But Simon Bunce lost his job, and his father cut off contact, when he was arrested after an ID fraudster used his credit card details on a child porn website.

[http://news.bbc.co.uk/2/hi/uk\\_news/magazine/7326736.stm](http://news.bbc.co.uk/2/hi/uk_news/magazine/7326736.stm)

**LexisNexis Data Breach Bigger Than Estimated.** Washington Post, April 13, 2005, Millions of consumers have been exposed to potential identity theft in 14 major breaches in the past year at various brokers, universities, banks and other institutions. Yesterday's announcement is a particularly harsh blow to the largely unregulated mega-brokers such as LexisNexis, ChoicePoint Inc. and Acxiom Corp [*or Verification Inc.*], which are part of a booming marketplace for personal data that also involves smaller resellers, marketers, some private investigators and others.

<http://www.washingtonpost.com/wp-dyn/articles/A45756-2005Apr12.html>

### **Privacy Breaches Expose Flaws in Laws**

<http://www.michaelgeist.ca/content/view/1626/159/>

Privacy took centre stage in Canada late last week as TJX Cos., the parent company of retail giants Winners and HomeSense, disclosed that as many as two million Canadian credit cards may have been accessed by computer hackers. Less than 24 hours later, the CIBC revealed that account information for 470,000 customers had been lost when a computer file went missing while in transit.

### **B.C. Hydro workers take preventative measures after theft of payroll**

**information,** The Province, Sunday, March 26, 2006, page A17

Some B.C. Hydro employees have had their bank accounts frozen after personal information - including salary and bank-account numbers of 4,200 company workers - [Laptop] was stolen from the offices of a private company contracted to handle the Crown Corporation's information databases.

### **Three million records lost in another UK government data scandal: And still no news on the 25 million missing child benefit records**

<http://www.computing.co.uk/computing/news/2205957/three-million-records-lost>

### **Government ID Card claims deflated; Biometric data open to abuse, says EU data supervisor, 2006**

[http://www.theregister.co.uk/2006/03/15/biometric\\_data\\_open\\_to\\_abuse/](http://www.theregister.co.uk/2006/03/15/biometric_data_open_to_abuse/)

Biometric data employed for identification purposes could be misused and lead to "function creep", the European Data Protection Supervisor has warned. The EDPS Peter Hustinx said the accuracy of biometric data in uniquely identifying a person is "overestimated", and could in fact "facilitate the unwarranted interconnection of databases".

### **Criminal Record; The Stain that won't go away** Toronto Star, 2008 (Employer 'paranoia' strikes people convicted or even just accused of a crime)

<http://www.thestar.com/SpecialSections/Crime/article/460766>

### Consent to and Authorization for Disclosure of Personal Information For Preparation of a Background Report for Employment Purposes

Through this document, it is being disclosed to me and I understand that a Background Report (also known as a **Consumer Report** or **Investigative Consumer Report**) may be prepared about me as part of my application for employment and/or continued employment. Further, I understand that information about me may be transferred to / from the US and retained in the US.

I authorize \_\_\_\_\_ to procure a Background Report from **Verifications, Inc.**, and I authorize Verifications, Inc., a US-based Safe Harbor Certified employment screening company (also known as a Consumer Reporting Agency) and its agents, to retrieve necessary information and prepare such Background Report. I understand that a Background Report may be prepared summarizing information from personnel files, educational institutions, government agencies, companies, corporations, credit reporting agencies, law enforcement agencies (including the *Royal Canadian Mounted Police* if permissible) at the international, federal, provincial or local level relating to my past activities. I authorize these entities to supply any and all information concerning my background. The information received may include, but is not limited to, academic, residential, achievement, job performance, attendance, litigation, personal history, credit reports, driving records, and criminal history records for which an absolute discharge or full pardon has not been granted. If my prior employers and/or references are contacted, the report may include information obtained through personal interviews regarding my character and general reputation. I understand and authorize that some or all of this information about me may be transmitted electronically and, when required, may be transferred across international borders. I understand that supplemental forms and/or authorizations may be required to obtain international information and that host-country and receiving country privacy laws will be observed if information is transferred across international borders.

I understand that this report, if prepared, will be compiled, disseminated and retained in compliance with all federal and provincial law, including but not limited to, the Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA) and applicable provincial privacy legislation, including the *Personal Information Protection Act* (British Columbia), the *Personal Information Protection Act* (Alberta), the *Act Respecting Personal Information in the Private Sector* (Quebec), applicable provincial health sectoral privacy legislation and other applicable law including the *US Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.*, and its State Analogues. I may request a copy of any report that is prepared regarding me and a copy of Principles Set Out in the National Standard of Canada Entitled *Model Code for the Protection of Personal Information, CAN/CSA-Q830-96* as contained in PIPEDA. I may request and have the right to receive the nature and substance of all information about me contained in the files of Verifications. I understand proper identification will be required and I should contact: **Verifications, Inc., 1425 Mickelson Drive, Watertown, SD 57201, USA. Phone 1-800-247-0717 / +1 605-884-1200**

Please contact Verifications at 1-800-247-0717 or the address above to request a copy of your Background Report.

*I authorize the above-named company to procure a Background Report about me from Verifications, Inc. I am willing that a photocopy of this authorization be accepted with the same authority as the original; and that if employed by the above-named company this authorization will remain in effect throughout such employment unless prohibited by applicable law or I withdraw my authorization in writing.*

Signature \_\_\_\_\_ Social Insurance Number \_\_\_\_\_ Date (Spell Month) \_\_\_\_\_

**NOTE:** Do not provide the following information until you have read and signed the *Consent to and Authorization for Disclosure of Personal Information* above. The information requested below is needed to conduct your background investigation and IS NOT considered part of your application. PLEASE PRINT CLEARLY.

Last Name	First Name	Middle Name	Date of Birth (spell month)
Street Address		City	
State/Province	Country		ZIP/Postal Code
Driver's License No.	Country/State/Province of License		Expires On

List any other COUNTRIES, CITIES, and PROVINCES/STATES in which you have lived during the previous 7 years

List any other LAST NAMES you have used during the previous 7 years

List any other LAST NAMES under which you received your GED, high school diploma, or other academic credentials.

**If you have experience or qualifications from outside Canada, please request and complete an International Supplement.**



## Medical Authorization Form

I/We authorize any health care professional, as well as any health or social service establishment, any insurance company, the Medical Information Bureau, financial institution, personal information agents or security agencies, my/our employer or any former employer and any public body holding personal information concerning me/us, particularly medical information, to supply this information to RBC Life Insurance Company and its reinsurers for the risk assessment or the investigation necessary for the study of any claim.

Such information will be provided for the following purposes: (a) assessment of insurance risk for underwriting purposes; (b) investigations necessary to adjudicate any claim or assess the validity of the policy as issued. For the same purposes, I/we authorize RBC Life Insurance Company, its reinsurers, and the Medical Information Bureau, to exchange the personal information contained in this application with other insurers, market intermediaries, financial institutions, and persons with whom I/we have indicated as references. I/We also authorize the Underwriting Department of RBC Insurance to release to my/our doctor(s) any medical results obtained as a result of my/our application for insurance for the purpose of assisting in explaining those results.

I/We authorize RBC Life Insurance Company, or its Reinsurer, to exchange the personal information contained in this application with other insurers, market intermediaries, financial institutions, or persons whom I/we have indicated as references and to inquire of them for the appraisal of the risk or in the event of a claim.

A photocopy of the signed authorization shall be as legally valid as the original.

Signed at \_\_\_\_\_ this \_\_\_\_\_ day of \_\_\_\_\_ 20 \_\_\_\_\_

\_\_\_\_\_  
Witness

\_\_\_\_\_  
Signature of Proposed Life Insured

**In Alberta only:** This authorization will be valid until revoked by written notice to RBC Life Insurance Company.

**RBC Life Insurance Company**

Calgary Office: 10655 Southport Road SW, Suite 600 Calgary Alberta T2W 4Y1 ~ 403-531-1764  
Mississauga Office: 6880 Financial Drive, West Tower, Mississauga, Ontario, L5N 7Y5 ~ 905-606-1000  
Montreal Office: 1 Place Ville-Marie, 13<sup>e</sup> étage nord, Montréal, Québec H3C 3A9 ~ 514-288-4309

## Your Privacy Matters To Us

At RBC Insurance<sup>®</sup>, we're committed to protecting your privacy. We respect your privacy and want you to understand how we safeguard your personal information.

### How we collect your information

We collect and keep information about you, which is needed to provide the products and services you request. We collect information from you, either directly or through our representatives. We may also need to collect information about you from sources such as hospitals, doctors and other health care providers, the Medical Information Bureau, the government (including government health insurance plans) and other governmental agencies, other insurance companies, financial institutions, motor vehicle reports, and your current and former employer.

### How we use your information

We use your information to provide the products and services you request, which includes using it to evaluate insurance risk and manage claims. We may also share your information with others who work for companies under RBC Insurance or other RBC Financial Group<sup>™</sup> companies, or with third parties, when it is necessary for the services we provide to you. Third parties may include other insurance companies, the Medical Information Bureau, financial institutions, third party administrators, and any references you provide.

We may use your information internally, to prepare statistical reports that help us understand the needs of our customers and that help us understand and manage our business.

If you have given us your social insurance number, we will use it for taxation purposes and to help identify you with Citizenship and Immigration Canada, when necessary.

---

*Please note that this paragraph is not applicable if this application is submitted by an independent representative or a representative that is attached to a firm other than RBC Insurance.*

### Other ways we may use your information

When you request products and services directly from a company under RBC Insurance, there are other ways we may use your information. For example, we may use or share some of your information to help you find out about other products and services from a company under RBC Insurance and other RBC Financial Group companies. However, we will never use or share your health information for these purposes. To better manage your relationship with other RBC Financial Group companies, and where the law allows us, we may consolidate the information we have about you with information held by the other companies.

If, at any time, you decide that you do not want us to use your information as described here, under "Other ways we may use your information", please let us know by calling us at 1-800-663-0417.

### Your right to access your information

You have a right to access the personal information that we have about you in your file. If we have information that is not correct, you can have it corrected.

To access your information or to ask us to correct information, you can contact us at:

#### **RBC Life Insurance Company**

**P.O. Box 515, Station A,**

**Mississauga, Ontario**

**L5A 4M3**

**Telephone: 1 800 663 0417**

**Facsimile: (905) 813 4816**

### If you would like more information about client privacy

RBC Financial Group publishes a brochure on client privacy. If you would like a copy of the brochure, you can contact us and we would be pleased to send one to you.