Respecting Privacy

A Compliance Review Tool for Manitoba's Information Privacy Laws

A Special Report

Prepared by:

Ombudsman Manitoba

October 2003

Ombudsman Manitoba

750 – 500 Portage Avenue
Winnipeg, Manitoba R3C 3X1
Telephone: (204) 982-9130
Toll Free in Manitoba
1-800-665-0531
Fax: (204) 942-7803
E-mail: ombudsman@ombudsman.mb.ca

500 av. Portage, pièce 750
Winnipeg (MB) R3C 3X1
Téléphone : (204) 982-9130
Sans Frais au Manitoba :
1-800-665-0531
Télécopieur : (204) 942-7803
Courriel : ombudsman@ombudsman.mb.ca

www.ombudsman.mb.ca

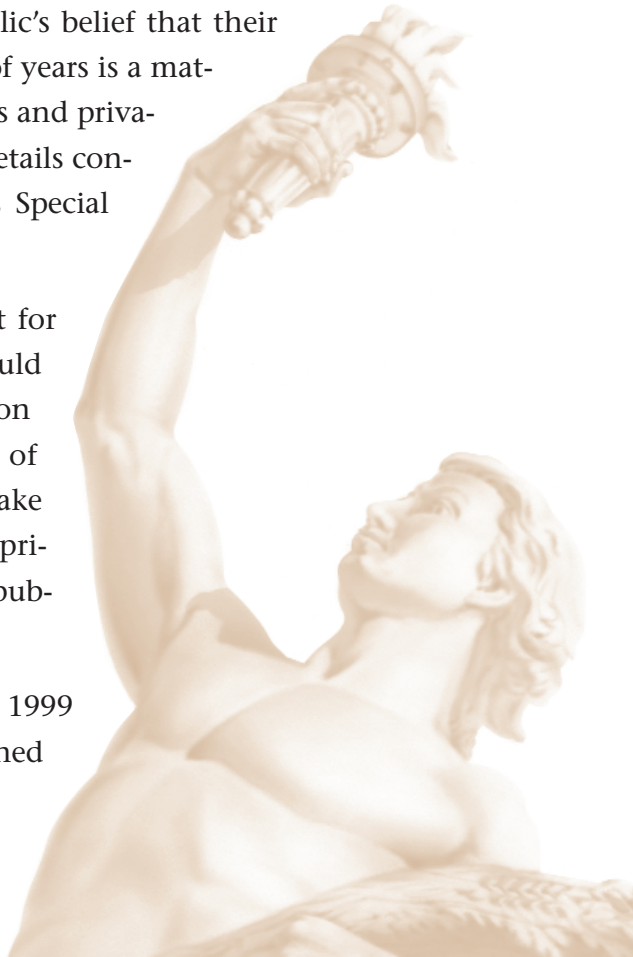
Letter of Transmittal

To the Members of the Manitoba Legislature:

It has been more than five years since the Manitoba Legislature passed *The Personal Health Information Act* (PHIA) and *The Freedom of Information and Protection of Privacy Act* (FIPPA). One of the principal lessons the Office of the Ombudsman has learned through its compliance oversight experience has been the need for public bodies and health information trustees to approach the management of personal information more systematically and proactively.

This need is underscored virtually on a daily basis as modern information and communication technologies facilitate the expanding collection, use, and disclosure of personal and personal health information.

Results of a recent survey that point to the Manitoba public's belief that their personal privacy has been eroded during the past number of years is a matter of concern, especially considering that Manitoba's access and privacy legislation came into force during this period. Further details concerning this survey are featured at the beginning of this Special Report to the members of the Manitoba Legislature.



The purpose of this Special Report is to provide a context for and to present a privacy impact assessment process that could significantly enhance both the real and perceived protection of the personal and personal health information of Manitobans. Use of this Privacy Compliance Tool will take resources and commitment, but the payoff will be better privacy protection and increased trust and confidence of the public in how their personal information is being managed.

In some respects, this Special Report is a follow-up to our 1999 report to the Legislature, *A Privacy Snapshot*, which we published

to provide a sense of the privacy environment with the coming into force of FIPPA and PHIA. What we said in the introduction to the Snapshot remains equally valid today:

> *With the accelerating advances in computing and electronic communications, personal information has become a focus of intense interest by many organizations and individuals for a variety of purposes ranging from commerce to research, from service to the public to public safety, and from personal to national security. It has been characterized as a commodity and the protection of it as a human right. While the proper use of personal information can be benign or even beneficial, the abuse of it can lead to consequences ranging from the merely irritating to the terrifying.*

Under section 58(3) of *The Freedom of Information and Protection of Privacy Act* and section 37(3) of *The Personal Health Information Act*, the Provincial Ombudsman may, in the public interest, publish a Special Report relating to any matter within the scope of the powers and duties of the Ombudsman. Among these responsibilities is a duty to inform the public about these two enactments. As well, the Ombudsman's Office serves as an oversight function concerning the collection, use, disclosure and security of personal information and personal health information.

Original signed by

Barry Tuckett
Ombudsman

RESPECTING PRIVACY

A Compliance Review Tool for Manitoba's Information Privacy Laws

Contents

What do Manitoban's Think About their Information Privacy?

Six out of every ten Manitobans believe that they have less personal privacy than just five years ago according to survey results released to the Office of the Manitoba Ombudsman by EKOS Research Associates.[1]

In fact, a majority of Manitobans hold the view that "real" personal privacy has become so eroded that it no longer exists in some respects. Specifically, 75% agree that there is "no real privacy" because the government can learn anything it wants about individuals. At least one in two Manitobans (55%) believe that it is more likely than not that they will suffer a serious invasion of privacy during the next two years.

The Manitoba Legislature passed *The Personal Health Information Act* (PHIA) and *The Freedom of Information and Protection of Privacy Act* (FIPPA) in June 1997 to protect the public's personal and personal health information. PHIA was proclaimed in December 1997 and FIPPA in May 1998.

EKOS survey results indicate that approximately seven in ten Manitobans are vaguely (26%) or clearly (35%) aware of laws that place strict restrictions on how provincial government departments are able to use or share their personal or personal health information. Nevertheless, Manitobans are cautious in their belief that these laws are being adhered to appropriately. About one in four (26%) report that they are highly confident that the Government will follow its own privacy laws. The remainder have low (19%) to moderate confidence (50%), or did not know or did not respond.

Considering that the provision of personal or personal health information is normally not a matter of choice for people in obtaining essential provincial public services and benefits, we find these figures to be a matter for concern. There should be a higher level of public trust and confidence in how personal and personal health information is handled by entities covered by Manitoba's privacy laws.

It is interesting to view the mandatory requirement for personal information in return for obtaining public services in a context that includes the marketplace, where consumers routinely expect options to be available for acquiring goods and services. In the private sector, no less than two-thirds of Canadians would stop shopping at a favourite store and three in four would consider switching their financial institution if they felt their information were being misused. Such options are not ordinarily available in the public sector.

A particularly disturbing survey finding, considering the implications, was that more than one in ten Manitobans (12%) have withheld personal information from a health care provider because of privacy concerns.

Such results underline a reality that the implications of a privacy breach, or simply the perception of a breach, have deeply significant consequences for individuals, businesses, and government.

1 EKOS Research Associates Inc., "The Rethinking the Information Highway Study", 2002-03 edition.

RESPECTING PRIVACY

A Compliance Review Tool for Manitoba's Information Privacy Laws

PERSONAL INFORMATION PRIVACY

Information privacy is an important matter of public policy as well as of law, principles, and practices.

Privacy is also a recurring topic of media coverage in North America and abroad. Not a single day goes by without our office receiving literally scores of reports from news services involving privacy issues, developments, concerns, and about breaches of the right to privacy touching people ranging in numbers from one to tens of thousands and more. The stories probably represent but a small proportion of the greater and lesser privacy violations that do not make the news in the course of a year. These reports remind us of the vulnerability and susceptibility of personal information to sometimes well-intentioned but ill-considered collections, uses, and disclosures; to theft and other unlawful practices; and to lax security measures.

While we do not take these news reports as a measure of personal information privacy protection in Manitoba, our experience suggests that it would be prudent, good practice, and in the public interest to ensure that the requirements of Manitoba's privacy legislation are better known, more fully considered, and more systematically applied than is now the case.

PURPOSE OF THIS SPECIAL REPORT

The purpose of this Special Report to the Members of the Manitoba Legislature is to present a privacy impact assessment process that we believe can significantly enhance protection of the public's personal and personal health information privacy under *The Personal Health Information Act* and *The Freedom of Information and Protection of Privacy Act*.

A privacy impact assessment is both a structured due diligence process and a personal information management diagnostic tool to assist organizations in reviewing their compliance with statutory privacy requirements and "best practices". Such an assessment requires a thorough analysis of an organization's policies and activities that have an impact on the information privacy of individuals.

The Privacy Compliance Tool being introduced here has been designed specifically for use under Manitoba's information privacy laws by public bodies and personal health information trustees to pinpoint any area of non-compliance that should be addressed to properly protect the privacy of individuals. It should be used by any entity that is developing or revising a program, a practice, legislation, information system, or embarking on any other initiative that involves identifiable personal or personal health information. It may also be used to review existing programs. A clear intention of Manitoba's legislation is to prevent breaches of information privacy before they occur to the extent possible. As many have said, once privacy is lost, it is lost, and little or nothing can be done to restore it.

Central purposes of FIPPA are to control the manner in which public bodies may collect personal information from individuals and to protect individuals against unauthorized use or disclosure of personal information by public bodies….

Central purposes of PHIA are to control the manner in which trustees may collect personal health information, to protect individuals against the unauthorized use, disclosure or destruction of personal health information by trustees [and]to control the collection, use and disclosure of an individual's PHIN….

A clear intention of Manitoba's legislation is to prevent breaches of information privacy before they occur….

ABOUT FIPPA AND PHIA:

The Freedom of Information and Protection of Privacy Act (FIPPA) and *The Personal Health Information Act* (PHIA) were passed by the Manitoba Legislature in June 1997. PHIA was proclaimed in December 1997 and FIPPA in May 1998. Protecting personal and personal health information privacy is a requirement in Part 3 respectively in each of these Acts.

The Government of Manitoba passed these laws to set out the requirements for managing personal and personal health information held by public bodies and trustees.

The Government of Manitoba passed these laws to set out the requirements for managing personal and personal health information held by public bodies and trustees.[2] The Acts prescribe a number of information management practices regarding the collection, use, disclosure, retention, and security of this information. In these statutes,

- ***personal information*** is recorded information about an identifiable individual including, for example, a person's name, address or home telephone number, age, gender, sexual orientation, marital or family status, religious belief or association, hereditary characteristics, education, employment, criminal history, an identifying number (e.g. case file number, credit card number or social insurance number), and financial and health information.

- ***personal health information*** is recorded information about an identifiable individual that relates to the individual's health, health care history, genetic information, the provision of and payment for health care, and includes the Personal Health Identification Number (PHIN) or other identifying particular assigned to the individual, and any identifying information that is collected in the course of and is incidental to the provision of and payment for health care.

THE PRIVACY COMPLIANCE TOOL

We are pleased to offer a Privacy Compliance Tool (PCT) that focuses on the provisions of FIPPA and of PHIA, the latter being the first of its kind in Canada to deal specifically with personal *health* information. These complementary statutes have a common base of internationally accepted principles of fair information practices. The PCT consists of a Privacy Compliance *Checklist* and a *Guide*. The *Guide* serves to remind users of the statutory requirements and identifies some best practices to assist in completing the *Checklist*. The *Checklist* provides organizations with a step-by-step self-assessment process covering the basic requirements of good information privacy practices.

The Privacy Compliance Tool is intended to fill what we see as a significant gap in the administration of Manitoba's information privacy regime.

The Privacy Compliance Tool is intended to fill what we see as a significant gap in the administration of Manitoba's information privacy regime. At the same time, we are conscious that our office cannot compromise its role as an independent and impartial oversight office by suggesting that its use will eliminate privacy risks and breaches. Nevertheless, it will certainly help organizations comply with the legislation and meet due diligence requirements. We encourage the use of this tool to assess existing programs or before proceeding with new programs, practices, systems, and initiatives that may have an impact on privacy. Additionally, familiarity with the PCT should help increase awareness and understanding of the personal information management rules implicated by FIPPA and PHIA. It will also assist our office in terms of reviewing compliance with the legislation.

2 PHIA encompasses health professionals such as doctors, dentists, physiotherapists, and chiropractors; health care facilities such as hospitals, medical clinics, personal care homes, community health centres, and laboratories; health services agencies that provide health care under an agreement with a trustee; and public bodies as defined under FIPPA. Public bodies include provincial government departments, offices of the ministers of government, the Executive Council Office (Cabinet), and agencies including certain boards, commissions or other bodies; local government bodies such as the City of Winnipeg, municipalities, local government districts, planning districts and conservation districts; educational bodies such as school divisions, universities and colleges; and health care bodies such as hospitals and regional health authorities.

To provide a flavour of the *Guide* and *Checklist*, we have attached a *Checklist at a Glance* as ***Appendix 1***. This document captures the structure of the full *Checklist*, includes all the questions and interrogative statements of the full *Guide* and *Checklist*, but does not provide the detailed explanatory notes, comments, definitions, statutory references or recommended best practices.

WHAT IS PRIVACY?

Privacy is a legal right and many believe that it is a fundamental human right. During the past decade or so, the concern for privacy has taken on increasingly complex dimensions as information networks have expanded our ability exponentially to access information. The particular aspect of privacy that relates to the collection, use, disclosure, storage, and general management of personal information is known as information privacy.

Privacy is a legal right and many believe that it is a fundamental human right.

The concept of information privacy recognizes an individual's right to determine when, how, and to what extent he or she shares personal information with others.

In order to maintain the trust and confidence of clients, employees, patients, and the public, it is essential that government, public bodies, and personal health information trustees respect the privacy and security of identifying personal and personal health information.

PRIVACY AND SERVICES TO THE PUBLIC

In recent years, we have noted a growing interest among Manitoba's public bodies and trustees in the development of a privacy compliance assessment tool specific to the Province's access and privacy legislation. Several other jurisdictions have developed privacy impact assessments as a critical methodology to identify privacy concerns and to mitigate risks and harms inherent in the collection, use, disclosure, and retention of personal information in the delivery of goods and services to the public in today's computing and communications environment.

Governments and health care providers deliver a wide range of services to the public. In the course of offering these services, they acquire and have custody or control of extensive and diverse quantities of personal and personal health information. This information often *must* be given by an individual in order to receive the service or benefit. The mandatory nature of such transactions between an individual and the service provider is moderated by the application of fair information practices[3] and information privacy laws passed by the Manitoba Legislature.

Under these principles and laws, the "exchange" of personal and personal health information for services is imbedded in a trust relationship that no more personal information will be collected, used, or disclosed than is necessary for providing a service or as permitted by law; that no one will have access to the information except on a need-to-know basis or as permitted by law; and that the information will retained, protected, and destroyed as permitted or required by law.

Privacy protection should be treated as a normal, routine, and fundamental part of corporate and operational planning.

3 In 1996, the Canadian Standards Association launched a Model Code for the Protection of Personal Information and subsequently adopted it as a "National Standard". This code is reproduced in summary form as Appendix 2 of this Special Report. This code provided much of the infrastructure of the federal government's Personal Information Protection and Electronic Documents Act (PIPEDA), which received Royal Assent in the year 2000. This Act will come into force On January 1, 2004, with respect to the collection, use, and disclosure of personal information in the course of any commercial activity in Manitoba, including provincially regulated organizations in the absence of "substantially similar" provincial legislation.

…the Privacy Compliance Tool is not intended to dislodge any effective instrument that is already in place, but we do invite public bodies and trustees to use it as a measure of or as a supplement to any existing tool.

FIPPA and PHIA were designed to protect personal and personal health information privacy, not to place obstacles in the way of achieving corporate and operational objectives. Privacy protection should be treated as a normal, routine, and fundamental part of corporate and operational planning. Use of this *Checklist* and *Guide* will help management, staff, and contracted agents build information privacy compliance into the everyday business of their organizations.

Some public bodies or personal health information trustees may have a privacy impact assessment template that they have used, but we do not know that this is the case. In any event, the Privacy Compliance Tool is not intended to dislodge any effective instrument that is already in place, but we do invite public bodies and trustees to use it as a measure of or as a supplement to any existing tool.

A BACKWARD GLANCE BEFORE MOVING ON

In 1999, the Manitoba Ombudsman issued his first Special Report to the Legislature by way of introducing the "lay of the land" in information privacy following the proclamation in of PHIA in December 1997 and FIPPA in May 1998.

Addressing the Members of the Manitoba Legislative Assembly through a Special Report entitled, *A Privacy Snapshot taken September 1999*,[4] the Ombudsman wrote:

> *In view of the many recent unprecedented, complex and dynamic privacy issues touching the public, government and our office, this Special Report has been prepared as a "Snapshot" of today's privacy environment.*

As we look back over the more than five years since FIPPA and PHIA came into force, the words of the 19th century French satirist Alphonse Karr come to mind in relation to our first Special Report: "The more things change, the more they stay the same."

September 11, 2001

No other event in recent years than the terrorist attacks in the United States on September 11, 2001, has focussed more clearly the tensions between civil rights and liberties and the needs for public safety and national security.

No other event in recent years than the terrorist attacks in the United States on September 11, 2001, has focussed more clearly the tensions between civil rights and liberties and the needs for public safety and national security. However, attributing the current unstable or – as some would say – embattled state of personal information privacy to these attacks would not recognize that many personal privacy issues had already reached a significant level of national and international exposure.

In the early 1970s, the use of what was then commonly called "automatic data processing" was spreading rapidly through public and private sector organizations. Some of the implications for privacy of this technology were soon realized in North America and Europe. At the same time, the convergence and integration of wired and broadcast communication technologies with data processing capabilities was also well underway, epitomized in some respects by today's Internet, which has moved from a limited to an open network for the transmission of information.

In 1980, the Organisation for Economic Co-operation and Economic Development (OECD) introduced *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*, which Canada adopted in 1984. These guidelines established what has become known as the principles of fair information practice that form the core of modern information privacy protection statutes in Canada and elsewhere.

4 Our Special Report to the Legislature, A Privacy Snapshot taken September 1999, provides information and commentary on the general privacy environment to the year 2000 and is available on our web site at: http://www.ombudsman.mb.ca/reports/snapshot.htm

By the year 2000, information and communication technologies in relation to privacy matters had become a multi-faceted subject of vigorous and even bitter international discussion and debate, especially in relation to their actual and potential uses for surveillance purposes. The events of 9/11 intensified rather than introduced the now familiar concerns about finding a reasonable relationship between privacy and public safety or security matters in the use of modern information and communication technologies.

The events of 9/11 intensified rather than introduced the now familiar concerns about finding a reasonable relationship between privacy and public safety or security matters in the use of modern information and communication technologies.

Information and Communication Technologies and Better Services

For the better part of the past three decades, the rapid and accelerating development of information processing and communications technologies have set the pace for a defining social, cultural, political, and economic characteristic of our time: globalization.[5] In this world view, almost everything can be seen as being connected and information knows no border whether geopolitical or technological.

In this world view ["Globalization"], ... almost everything can be seen as being connected and information knows no border whether geopolitical or technological.

Organizations, including governments, have long recognized and responded to a variety of pressures to provide their goods and services more efficiently and effectively. The better use of information has often been touted as the master key to better services. In recent decades, the rapid and pervasive development of Information and Communication Technologies (ICTs) has been described as exerting a compelling "push" for the wider use of the technologies themselves, with applications for business and program purposes providing an intensifying or reinforcing "pull".

There is no doubt that ICTs have already provided important benefits for the provision of public services in – to name but a few – health, education, social assistance, agriculture, the workplace, environment, and law enforcement. Many service providers believe that these achievements are not much more than early explorations or harbingers of future applications of ICTs that will enhance service delivery.

The "Want" or "Need" to Use Personal Identifying Information

In this dynamic situation, where, one way or another, people are at the centre of the reasons for organizations existing, the pressure is intense to use personal identifying information as the essential means of making sense of and using the vast amounts of data available. Even at the current level of development and integration of information processing and communications technologies, it no longer seems farfetched to believe that the time is near when any random bit of recorded or transmitted information about anyone, anywhere could be brought together with other bits and sent anywhere at any time to provide an astonishingly complete picture of that individual in a record or in real time.

...the pressure is intense to use personal identifying information as the essential means of making sense of and using the vast amounts of data available.

The immense volume of personal information already being managed electronically by the health care and public sectors in Canada would, if held in paper form, require literally scores of records warehouses – more likely hundreds. This spatial concentration of information underlines the compelling and urgent need for organizations to be in full command of their personal information collection, use, disclosure, retention and security practices. Otherwise the risks of privacy breaches are significantly magnified over those relating to paper-held records.

[The]... concentration of [electronic] information underlines the compelling and urgent need for organizations to be in full command of their personal information collection, use, disclosure, retention and security practices.

5 This complex and multidimensional concept has been defined by the Canadian Government as describing "the increased mobility of goods, services, labour, technology and capital throughout the world. Although globalization is not a new development, its pace has increased with the advent of new technologies, especially in the area of telecommunications." (See: http://canadianeconomy.gc.ca/english/economy/globalization.html)

Federal and provincial governments everywhere in Canada are already using or implementing or examining ICTs with the avowed purpose of providing better, more economical, and effective services in most areas of their jurisdictions. A particularly notable example is the prospective development of a pan-Canadian Electronic Health Record.[6] The establishment of such a health information network has been the subject of study and recommendations for some years and appears to be on the verge of getting underway in earnest. Expected to cost in the billions of dollars, we could anticipate the development this EHR to be a matter of significant public consultation and discussion in the near future.

The establishment of [a pan-Canadian Electronic Health Record]...has been the subject of study and recommendations for some years and appears to be on the verge of getting underway in earnest.... Public trust and confidence in the information privacy protections underlying such a project will be key enabling factors in making it a success.

Public trust and confidence in the information privacy protections underlying such a project will be key enabling factors in making it a success. Central to the public's view will be assurance that all parties involved in the EHR comply with information privacy laws, principles, and policies relating to the collection, use, disclosure, retention, and security of the personal health information utlilized.

DUE DILIGENCE AND RISK MANAGEMENT

Among other things, a privacy compliance review is an effective due diligence and risk management process requiring direction and commitment from the executive level of organizations.

Among other things, a privacy compliance review is an effective due diligence and risk management process requiring direction and commitment from the executive level of organizations. While the need to undertake a review may be identified at any organizational level, the end product should be to provide the results of the assessment for executive review, sign-off, and decision-making for any actions or direction that may result, thus closing the accountability loop.

Conducting a thorough privacy compliance review in the early stages of developing or modifying a program, practice, system or legislation can help ensure that privacy requirements are identified and satisfied in a timely and cost-effective manner....

This Privacy Compliance Tool may be used as the foundation to assess the information privacy compliance of existing programs. It is especially timely to conduct a review when a new program, practice, information system or legislation is under development or is being modified if that program or system collects, stores, uses, or discloses personal or personal health information. Conducting a thorough privacy compliance review in the early stages of developing or modifying a program, practice, system or legislation can help ensure that privacy requirements are identified and satisfied in a timely and cost-effective manner, that privacy-invasive initiatives are not implemented, that privacy breaches are avoided to the extent possible, and that organizations are not faced with having to undertake expensive revisions or even to cancel a costly initiative after implementation.

RISKS ASSOCIATED WITH NOT CONDUCTING A PRIVACY ASSESSMENT

The general risks associated with failing to undertake a systematic privacy assessment are typically categorized as follows:

- Foremost is the risk for the information privacy of individuals in the knowledge that once privacy has been lost, it usually cannot be fully reinstated.

6 Manitoba was in the forefront of governments in Canada to embark on a major project to establish a Health Information Network. Announced in 1994, it was cancelled in 2000 without having achieved its main objective of suppling health care providers with easier and faster access to a substantial range of vital patient information. The prospective development of a Manitoba Health Information Network was a primary motive behind the province having the distinction of passing the first dedicated personal health information protection statute in the country: The Personal Health Information Act. Notably, the fourth clause of the preamble to the Act reads: "…clear and certain rules for the collection, use and disclosure of personal health information are an essential support for electronic health information systems that can improve both the quality of patient care and the management of health care resources".

- The program or legislative initiative may be brought into discredit with a significant and sometimes even a critical loss of public trust and confidence in an organization's regard for or consideration of the public's legal rights.
- Electronic systems in particular, but also programs, may have to be reconsidered, redesigned, or retro-fitted at substantial cost.
- Personal or personal health information is disclosed or "shared" through existing agreements that may not comply with the legislation or "best practices", or without any written agreement at all.
- Liabilities may ensue for employees and the organization.

USING THE PRIVACY COMPLIANCE TOOL

Undertaking a full privacy compliance review usually requires commitment from the organization involved. For this reason, we reiterate the importance of obtaining senior-level guidance and direction from the outset, bearing in mind that the results should be signed-off by executive decision-makers.

A thorough compliance review may well be an onerous task whose degree of difficulty will be influenced by a number of factors in addition to senior management commitment to fair information practices. These include the privacy expertise available in or to the organization; the extent to which personal and personal health information is collected, used, and disclosed by programs and information systems; the sensitivity of the information involved; the quality, currency, and pervasiveness of effective recordkeeping and information management practices; and the magnitude of the operation or programs involved.

Use of the Checklist will help entities subject to FIPPA and PHIA identify policies, processes, and organizational structures that are not responsive to the requirements of the legislation and to develop plans to bring non-compliant programs, practices, activities, and information systems into conformity with information privacy requirements.

Use of the Checklist will help entities ... bring non-compliant programs, practices, activities, and information systems into conformity with information privacy requirements.

The Checklist contains the considerations for assessing compliance and may be used by the Ombudsman's Office as a guideline for privacy audits or investigations. Using a privacy impact assessment process will help minimize information privacy breaches, but it may not entirely remove risk even when the overall scheme of a program or legislative proposal appears to comply with statutory requirements. Specific breaches will, unfortunately, occur from time-to-time and will have to be dealt with on a case-by-case basis. Nevertheless, a resulting compliance review or investigation by the Ombudsman will take account of the degree of due diligence having been practised through the employment of a privacy impact assessment.

Appendix 1

PRIVACY COMPLIANCE TOOL

CHECKLIST AT A GLANCE

INTRODUCTION

The purpose of this summary form of the larger *Checklist* is to provide users with a quick overview of the questions included in the privacy assessment. This document will facilitate keeping a record of answers and assessing overall compliance.

TABLE OF CONTENTS

ELEMENT 1

Identifying Purposes and Limiting Collection of Personal Information and Personal Health Information

\# Legend[1]:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

	Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. There is a detailed description of the type of *personal information*, *personal health information*, or personal data elements collected for this program or initiative.						
2. The purpose for collecting this *personal information* is authorized according to FIPPA. It is one of the following:† a. authorized by an enactment of Manitoba or Canada, or b. directly related to and is necessary for a program or activity of the *public body*, or c. necessary for law enforcement or crime prevention.						
3. *Personal health information* is not collected unless it is: a. for a lawful purpose connected with a function or activities of the *trustee*; and, b. is necessary for that purpose.						
4. *Personal information* or *personal health information* is collected only directly from the subject individual or his or her authorized representative.						
5. If *personal information* or *personal health information* is collected indirectly (i.e. from a third party), the *indirect collection* is authorized under Section 37(1) of FIPPA or Section 14 of PHIA.						
6. Individuals are informed (notified) of the purpose, authority (where FIPPA is involved) for *collection*, and how to contact an officer or employee who can answer their questions about *collection*.						

† **NB:** Please specify whether (a), (b), or (c) applies. If it is (a), identify the enactment(s) and applicable section(s).

1 Attachments offer additional information on what exists (e.g. a security policy) whereas Action Plans provide details on corrective or developmental actions that need to be taken (e.g. develop a training program to provide privacy and security awareness for staff).

ELEMENT 2

Limiting Use, Disclosure and Retention of Personal Information and Personal Health Information

Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

		Expl?		A/AP?	
	Y	N	Y	N	Y	N
A. Limiting Use						
1. *Personal* or *personal health information* is used only for the purpose for which it was obtained or for a use consistent with that purpose under FIPPA or directly related to that purpose under PHIA.						
2. *Consent* is obtained from the individual before using *personal information* for a purpose NOT consistent with the purpose for which it was collected or, in the case of *personal health information*, for a purpose NOT directly related to the purpose for which it was collected.						
3. There is a list of the staff position or categories that *use* this collection of *personal* or *personal health information*.						
4. Physical, administrative, and technical controls limit access to identifiable *personal* and *personal health information* to those who have a "need to know".						
5. The least amount of *personal information* and *personal health information* is used to meet the stated purpose.						
6. *Personal* or *personal health information* is used with the highest degree of *anonymity* to meet the stated purpose.						
B. Limiting Disclosure						
1. Individual consent is obtained before disclosing *personal* or *personal health information* to another government department or agency, *local public body*, *trustee* or other third party.						
2. If *consent* is not obtained, the *disclosure* is authorized according to a specific provision of Section 44(1) of FIPPA or Section 22(2) of PHIA.						
3. When *disclosure* is required and authorized, the amount and type of information disclosed is limited on a "need to know" basis.						
4. *Disclosure* is made at the highest degree of *anonymity* possible while still meeting the purpose of the recipient.						
5. Staff maintains a *disclosure* log or audit trail of:						
a. what information has been disclosed,						
b. to whom it has been disclosed, and						
c. the purpose and authority for the *disclosure*.						

 # LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

	Expl?		A/AP?	
	Y	N	Y	N	Y	N

C. Uses and Disclosures of Personal Information Not Otherwise Authorized under Division 3 of FIPPA

1. **For a *public body*** other than a *local public body* under Section 46 of FIPPA:
   The proposal or request has been referred to the Privacy Assessment Review Committee (PARC) for its advice:

   a. if the proposed *use* or *disclosure* is not otherwise authorized under Division 3, and involves *data linking* or *data matching* of *personal information* in one database with another, or

   b. if the request is for *disclosure* on a bulk or volume basis of *personal information* in one public registry or another collection of *personal information*.

2. **For a *local public body*** under Section 46 of FIPPA:
   The proposal or request has been either assessed internally by the *local public body* or referred to the Privacy Assessment Review Committee (PARC) for its advice:

   a. if the proposed *use* or *disclosure* is not otherwise authorized under Division 3, and involves *data linking* or *data matching* of *personal information* in one database with another, or

   b. if the request is for *disclosure* on a bulk or volume basis of *personal information* in one public registry or another collection of *personal information*.

3. For the *uses* or *disclosures* contemplated under Section 46 of FIPPA, the Head of the *Public Body* or *Local Public Body* has considered advice received through the statutory privacy assessment review process and approved conditions that must be met under Section 46(6), including a written agreement with the recipient of the *personal information*.

D. Disclosure of Personal Information for a Research Purpose under FIPPA

1. The Head of the *Public Body* or *Local Public Body* has considered any privacy assessment advice requested under Section 47(2) of FIPPA and approved conditions that must be met under Section 47(4), including a written agreement with the recipient of the *personal information*.

 # LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

		Expl?		A/AP?	
	Y	N	Y	N	Y	N
E. Disclosure of Personal Health Information for a Research Purpose under PHIA						
1. The *personal health information* required for the health research project is recorded information about an identifiable individual that relates to:						
a. the individual's health, health history (including genetic information about the individual), or						
b. the provision of health care to the individual, or						
c. the payment of health care provided to the individual, *and includes*						
d. the Personal Health Identification Number (PHIN) and any other identifying number, symbol or particular assigned to an individual, and						
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. The health research project has been approved according to the requirements of PHIA Section 24 by:						
a. the Health Information Privacy Committee (HIPC) if the *personal health information* is maintained by the government or a government agency, or						
b. an institutional research review committee if the *personal health information* is maintained by a *trustee* other than the government or a government agency.						
3. The researcher and the *trustee* have entered into an agreement under PHIA Section 24(4), and any regulations, in which the researcher agrees:						
a. not to publish the *personal health information* in an identifying form,						
b. to use the *personal health information* only for the purposes of the approved research project,						
c. to ensure that reasonable safeguards are in place to protect the security and *confidentiality* of the *personal health information*, and						
d. to ensure that the information will be destroyed or deidentified at the earliest opportunity consistent with the purposes of the project.						
F. Limiting Retention:						
1. There is a written records/data retention policy that meets all relevant legislative requirements.						
2. *Personal information* and *personal health information* used to make a decision that directly affects an individual are retained for a reasonable period of time to allow the individual to obtain access to it.						

ELEMENT 3

Ensuring Accuracy of Personal Information and Personal Health Information

 # Legend: "Y" = Yes; "N" = No; "Expl?" = Explanation?; "A/AP?" = Attachment or Action Plan?

			Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. There are procedures in place to verify *personal* or *personal health information* and to manage requests for corrections that comply with FIPPA Sections 38 and 39 or with PHIA Sections 16 and 12.						
2. The authority to modify or correct *personal* or *personal health information* is clearly established to ensure that those without this authority may not or are unable to alter these records.						
3. An audit trail is maintained to document when and by whom a file or record was compiled or updated.						

ELEMENT 4

Safeguarding Personal Information and Personal Health Information

Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

#		Y	N	Expl? Y	Expl? N	A/AP? Y	A/AP? N
1.	Security measures are in place for *personal* and *personal health information* regardless of media format (i.e. paper, photographic, electronic, etc.).						
2.	Written information security policies include a definition of roles and responsibilities, and sanctions for breaches of policy.						
3.	Staff receives ongoing training about security policies and procedures, and is made aware of the importance of security and *confidentiality* on an ongoing basis.						
4.	Security breaches and violations are documented and responded to according to established processes.						
5.	Access to *personal* or *personal health information* is regularly monitored and audited.						
6.	*Personal* and *personal health information* are stored or maintained in a physically secure location.						
7.	*Personal* and *personal health information* in all media are disposed of securely to prevent unauthorized access.						
8.	Physical removal of *personal* and *personal health information* of any medium from a secure designated area is always undertaken in a manner and in accordance with procedures that continue to ensure the security of the information at all times.						

LEGEND:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

ELECTRONIC SYSTEMS SECURITY:

			Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. Users are assigned unique user identifications and passwords for access to *personal* and *personal health information*, and passwords are changed regularly.						
2. Network and application security status is assigned on a "need to know" basis according to the particular requirements of specific roles within the organization.						
3. Access privileges are revoked promptly when required (e.g. when an employee leaves or moves).						
4. Systems contain audit trails for tracking data access, and audit logs provide information about abnormal or unusual access.						
5. Access logs and audit trails are reviewed on a regular basis.						
6. *Personal* and *personal health information* is transmitted by secure means to minimize opportunities for unauthorized or accidental interception by third parties.						
7 Virus protection is implemented and an effective firewall is in place where necessary, for all information systems that contain *personal* or *personal health information*.						
8. External providers of information management or technology services are covered by written agreements dealing with risks including unauthorized access, *use*, *disclosure*, retention, and destruction or alteration as required under FIPPA Section 44(2) and PHIA Section 25(3).						

ELEMENT 5

Ensuring Individual Access to Personal Information and Personal Health Information

Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

		Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. A process to respond to access requests under the Act(s) is in place.						
2. Individuals are informed that the organization holds *personal* or *personal health information* about them and that access to that data is provided, except in limited circumstances as defined in legislation.						
3. Requests for access are responded to within the legal time limits at minimal or no cost, or in compliance with legislation.						
4. The requested information is provided in an understandable format and the organization is prepared to explain any terms or abbreviations.						
5. A refusal to grant access to all or part of an individual's information includes clear reasons for the refusal.						

ELEMENT 6

Challenging Compliance

Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

		Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. There are communication policies and procedures in place that ensure individuals are routinely informed that they may make a complaint to the organization and are informed about their statutory right to make a complaint to the Manitoba Ombudsman respecting their *personal* and *personal health information* rights.						

ELEMENT 7

Accountability and Openess of Policies and Practices

Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

			Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. It is understood and known in the organization that the Head of a provincial government department or agency, or the Head of a *local public body*, or a *trustee* is accountable for compliance with access and privacy legislation, and that any delegation of powers and duties should be formally recorded.						
2. An employee (or employees) within the organization is formally delegated responsibility for the daily administration of privacy compliance ("access and Privacy coordinators" under FIPPA, "privacy officer" under PHIA). The identity of the individual(s) is known throughout the organization.						
3. There are written organizational policies and procedures that define the responsibility for protecting *personal* and *personal health information*.						
4. Appropriate staff is provided with on-going training to implement privacy policies and procedures.						
5. Other parties, such as information managers and agents, who may have authorized access to *personal information* or *personal health information* under Parts 3 of FIPPA and PHIA are aware of, and comply with, organizational privacy policies and relevant procedures.						
6. Individuals can obtain information about privacy policies and procedures with reasonable ease.						
7. Under FIPPA, *Personal Information Banks* have been identified, described, are up-to-date, and publicly available as required. [Note that PHIA does not have a corresponding provision in relation to production of a directory including a description of personal information banks.]						
8. Under FIPPA and in the case of a public body that is not a local public body, (1) a record is kept of uses and disclosures not included in the publicly available "Access and Privacy Directory", (2) this record is attached or linked to the personal information involved, and (3) a process is in place to have this information included in the "Access and Privacy Directory". [Note that PHIA does not have a directly corresponding provision.]						
9. A procedure exists for responding to questions or concerns about privacy practices.						

ELEMENT 8[8]

Assessing Privacy Risks in Electronic Service Delivery (ESD)

Legend:

"Y" = Yes; "N" = No; "Expl?" = Explanation?;
"A/AP?" = Attachment or Action Plan?

	Expl?		A/AP?	
	Y	N	Y	N	Y	N
1. Are diagrams available to illustrate the flow of *personal* and *personal health information* for this project?						
2. Has responsibility for control and custody for all *personal* or *personal health information* processed by the ESD system been identified and assigned?						
3. If the ESD system will process transactions for more than one program, agency or department, have constraints been placed on data integration?						
4. If this ESD project involves the use of common identifiers or a common identification infrastructure, have privacy-enhancing measures been considered to limit risk to privacy?						
5. Will this ESD initiative require *data linking* (data profiling) or *data matching*?						
6. Is there a means of obtaining, authenticating, registering and maintaining individual *consent* electronically, where required?						
7. Have privacy-enhancing technologies and/or techniques been considered for this ESD project?						
8. Have all risks to privacy for this ESD initiative been identified and documented?						
9. Have all risks to privacy for this ESD project been minimized or averted?						
10. Has a comprehensive risk analysis been undertaken to identify and implement appropriate ongoing monitoring and regular auditing requirements to protect *personal* and *personal health information*, including that of end-users, for all aspects of the ESD system?						
11. Have key stakeholders been consulted about the privacy implications of this project?						
12. Where risks to privacy are not completely mitigated, is there a strategy for responding to public concerns over privacy protection?						
13. Have constraints been placed on ESD service providers regarding the *collection*, *use* and *disclosure* of information subject to FIPPA and PHIA?						
14. Do all contracts related to the implementation of this ESD project contain data protection provisions?						

8 Users are asked to provide **Explanations and/or Action Plans** for ALL questions contained in this Element, regardless of a "yes" or no" response. **Attachments** offer additional information on what exists (e.g. a security policy) whereas **Action Plans** provide details on corrective or developmental actions that need to be taken (e.g. develop a training program and provide privacy and security training for staff).

Appendix 2

PRINCIPLES OF FAIR INFORMATION PRACTICES

Canadian Standards Association Principles in Summary Model Code for the Protection of Personal Information (1996)

1. Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes

The purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by lawful means.

5. Limited Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other that those which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.