

PHIA Privacy Compliance Tool

Guide

PHIA PRIVACY COMPLIANCE TOOL

GUIDE

PREFACE

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 that relates specifically to the Province's access and privacy legislation. Several other jurisdictions have developed Privacy Impact Assessments as a methodology to identify privacy concerns and to mitigate risks and harms inherent in the collection, use, disclosure, and retention of personal health information in the delivery of goods and services to the public in today's computing and communications environment.

We originally developed a Privacy Compliance Tool to encompass the provisions of *The Freedom of Information and Protection of Privacy Act* (FIPPA) and of *The Personal Health Information Act* (PHIA), complementary legislation that deals specifically with personal *health* information. Both statutes have a common base of internationally accepted principles of fair information practices.

To assist trustees who manage personal health information, we are pleased to offer a separate diagnostic tool that focuses specifically on PHIA compliance issues. Public bodies dealing with personal health information and personal information should use the original tool to assess their compliance under both statutes.

The PHIA Privacy Compliance Tool consists of a "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 privacy and security practices.

We have produced this "Checklist" and "Guide" 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 their use will eliminate privacy risks and breaches. Nevertheless, they will certainly help trustees comply with the legislation and meet due diligence requirements. They will also provide our office with an important investigative framework. We encourage the use of this tool to assess existing programs or before proceeding with new programs, systems, and initiatives that may have an impact on privacy. The "Guide" should help increase understanding and awareness of the personal health information management rules implicated by PHIA.

PHIA was designed to protect 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 and fundamental part of business planning. Use of this "Checklist" and "Guide" will help trustees, management, staff, information managers, and other contracted agents build information privacy compliance into the everyday business of their organizations.

In providing this compliance review process as part of the privacy tool kit available for Manitoba, we see it as a work in progress. We welcome comments about its application and utility with an eye to improving its content.

TABLE OF CONTENTS

GUIDE TO THE PHIA PRIVACY COMPLIANCE TOOL:

PREFACE	3
INTRODUCTION	
What is Privacy?	6
What is Personal Health Information and Personal Information?.....	6
About FIPPA and PHIA	6
Due Diligence and Risk Management.....	6
Risks Associated with Not Conducting a Privacy Assessment	7
Information Sharing Agreements	7
Research and Personal Health Information Privacy.....	7
The Ombudsman’s Office and Compliance Oversight	8
Using the PHIA Privacy Compliance Tool	8
Some Words about the Preparation of this Guide and Checklist	9
Some Helpful Web Site Links.....	10
ELEMENT 1: Identifying Purposes and Limiting Collection of Personal Health Information	12
ELEMENT 2: Limiting Use, Disclosure and Retention of Personal Health Information	15
ELEMENT 3: Ensuring Accuracy of Personal Health Information	19
ELEMENT 4: Safeguarding Personal Health Information.....	21
ELEMENT 5: Ensuring Individual Access to Personal Health Information	24
ELEMENT 6: Challenging Compliance	25
ELEMENT 7: Accountability and Openness of Policies and Practices.....	26
ELEMENT 8: Assessing Privacy Risks in Electronic Service Delivery	28
APPENDICES	
Common Terms and Definitions	31
Elements of Consent under PHIA: <i>Personal Health Information</i>	34

INTRODUCTION¹

WHAT IS PRIVACY?

Privacy is important. It is a legal right and many believe that it is a fundamental human right. Over the past decade or so, the concern for privacy has taken on increasingly complex dimensions as information networks have increased 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.

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

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

WHAT IS PERSONAL HEALTH INFORMATION AND PERSONAL INFORMATION?

Personal health information is information about an individual collected or created during the provision of health services. Examples of *personal health information* include an individual's name, address, telephone number, a Personal Health Identification Number (PHIN), diagnosis and treatment information. For more complete definitions, see the "Common Terms and Definitions" section at end of this "Guide".

Personal information is any recorded information about an identifiable individual. Examples include a person's name, address, or telephone number, a number that can identify them (e.g. case file number, credit card number or social insurance number), and financial and health information. For the full statutory definition, see the "Common Terms and Definitions" section at the end of this "Guide".

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 of FIPPA and Part 3 of PHIA. The Government of Manitoba passed these complementary laws to set out the requirements for managing *personal* and *personal health information* held by *public bodies* and *trustees*.² The Acts describe specific information management practices regarding the *collection, use, disclosure, retention, and security* of this information.

It is important to note that FIPPA does not apply to a person's access and privacy rights to his or her own personal health information. These rights are contained in PHIA.

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. While the need to undertake a review may be identified at any organizational level, the end product should be to

¹ Please note that throughout the text of the "Checklist" and "Guide", certain words or terms may be italicized to indicate that they are defined in *Appendix I* to the "Guide". Italics are also used for some subheadings and for references to statutes.

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.

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.

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, system or legislation is under development or is being modified if that program or system collects, stores, uses, or discloses *personal health information*. Conducting a thorough privacy compliance review in the early stages of developing or modifying a program, 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 costly revisions or even to cancel a costly initiative after implementation.

RISKS ASSOCIATED WITH NOT CONDUCTING A PRIVACY ASSESSMENT

The general risks normally 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.
- 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 retrofitted at substantial cost.
- *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.

INFORMATION SHARING AGREEMENTS

"Information sharing" is a commonly used concept or term for the exchange, *collection* or *disclosure* of *personal health information* by a party in one jurisdiction with a party in another jurisdiction or a non-public entity for certain purposes. This concept is also commonly incorporated into a so-called *Information Sharing Agreement* between or among parties within or outside Manitoba. Information sharing is not a term to be found in PHIA.

The provision of *personal health information* by a trustee to another jurisdiction, non-public entity, or another trustee should be considered as a *disclosure*. Similarly, the receipt of *personal health information* through an Information Sharing Agreement should normally be considered a collection. Because of the widespread use of the term, it will be used from time-to-time in the "Guide" and "Checklist", but it should be understood in the context of the general and specific requirements of PHIA (see PHIA sections 22(2)n and 22(2)o).

PHIA includes specific regulation-making power respecting written agreements involving certain uses and disclosure of *personal health information*, but none have been issued as of Spring 2004.

RESEARCH AND PERSONAL HEALTH INFORMATION PRIVACY

PHIA regulates the *collection, use, disclosure, security, retention and destruction* of *personal health information*. It is important to note that *personal health information*, by definition, includes "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". (PHIA Section 1)

Approval for a health research project involving the *disclosure* of identifying *personal health information* must be obtained under Section 24 of PHIA. Approval may be given by the Health

Information Privacy Committee (HIPC) established under the Act (Section 59) if the information is maintained by the government or by a government agency. If the information is maintained by a trustee other than the government or government agency, approval may be given by an institutional research review committee.

Approval of a health research proposal includes a determination that:

- the research is important enough to outweigh any invasion of privacy involved,
- the research cannot be done without using identifiable *personal health information*,
- it is impossible or impractical to get *consent* from the people the personal health information is about,
- the project ensures the security of the personal health information and its destruction when finished, and
- all identifying information will be removed as soon as possible consistent with the purposes of the project.

Approval is conditional on a written agreement between the *trustee* and the researcher, which includes undertakings that:

- the *personal health information* will not be published in an identifiable form,
- it will be used only for the purposes of the approved project, and
- the information will be kept securely and only for as long as is necessary for purposes consistent with the project.

THE OMBUDSMAN'S OFFICE AND COMPLIANCE OVERSIGHT

The Ombudsman heads the Office of the Legislature that, among other things, reviews compliance with access to information and privacy rights under PHIA. Under this legislation, the Office is mandated to investigate and initiate complaints. In addition to other general powers and duties, the Ombudsman may comment on the implications for access to information or protection of privacy of proposed legislative schemes or programs of trustees and on the implications for the protection of privacy of:

- (i) using or disclosing personal health information for record linkage; or,
- (ii) using information technology in the collection, storage, use, or transfer of personal health information. (PHIA Section 28 (d) and (e))

USING THE PHIA PRIVACY COMPLIANCE TOOL

Undertaking a full privacy compliance review normally 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 health information* is collected, used, and disclosed by programs and information systems; the sensitivity of the information involved; the quality, currency, and pervasiveness of sound recordkeeping and information management practices; and the magnitude of the operation or programs involved.

The privacy requirements in this tool are classified and organized by practice, and provide a generic approach to privacy assessment and compliance. For the convenience of users, the "Guide" provides in whole or in part, some of the sections of the legislation. This has contributed substantially to the size of the "Guide" and carries the risk of inadvertently lulling users into relying more on these isolated

sections than on their own reading of legislation and neglecting the general rule that the law should be read as a whole.

Use of the “Checklist” will help trustees under 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, activities, and information systems into conformity with information privacy requirements. We have provided the “Checklist” in summary form (“Checklist at a Glance”) as an overview of the process and a tally of responses to the questions.

An information privacy assessment should be undertaken prior to the development of Electronic Service Delivery (ESD) systems, legislation, and policy or program implementation where *personal health information* is involved. Proposals for ESD, for example, should include the assessment as part of the package presented to systems designers so that privacy issues are clearly identified. It is not the primary responsibility of systems designers to conduct the privacy impact assessment. This responsibility belongs principally to the entities holding personal health information. Use of this “Checklist” and “Guide” is based on this premise, and is not aimed at the technical detail best addressed by electronic systems planners and designers.

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 practiced through the employment of a privacy impact assessment.

SOME WORDS ABOUT THE PREPARATION OF THIS GUIDE AND CHECKLIST

In preparing this “Checklist” and “Guide”, we consulted extensively with other jurisdictions -- both on the administrative and the oversight sides -- which use such instruments. There was complete agreement on the importance of conducting such privacy impact assessments and on the reality that there is no “silver bullet” providing a simple and quick analysis of privacy compliance in existing or proposed programs and activities. There are also several schools of thought about how detailed such assessments should be. If they are very detailed, users find them somewhat daunting to undertake; if they are too simple, they do not do the job and the results can be misleading.

Oversight offices tended to prefer the more detailed version because of the nature of their work, as did some of the larger and more experienced users. Offices charged with administration of privacy legislation generally advocated the simpler – not to say simplistic – versions on the grounds that there is a better chance that they will be employed. There were also several differing opinions about the scope of such tools including the suggestion that one instrument could not easily do the job for both existing and proposed programs and activities. Nevertheless, there was general agreement that the most challenging and widespread need was for the review of existing programs, and that the use of privacy impacts was absolutely essential as part of the development of new programs.

The “Checklist” and “Guide” have been prepared to be applicable for both existing and new programs. We hope the flexibility of electronic formats will enable users to adapt the tool in some respects to their own organizational needs.

SOME HELPFUL WEB SITE LINKS

Further information about Manitoba’s access and privacy legislation is available on web sites maintained by Manitoba Health (for PHIA) and Manitoba Culture, Heritage and Tourism (for FIPPA). These sites do not deal with privacy impact assessments, but do provide a wealth of other information about the legislation.

The Manitoba Ombudsman's Office also has a web site focussing on PHIA and FIPPA.

Information about what some other jurisdictions are doing by way of privacy impact assessments may be found at the web sites listed following Manitoba below.

■ **MANITOBA – PHIA:**

- Manitoba Health, Legislative Unit:
<http://www.gov.mb.ca/health/phia/index.html>
- Manitoba Health, Health Information Privacy Committee:
<http://www.gov.mb.ca/health/hipc/index.html>
- Office of the Manitoba Ombudsman, Access and Privacy Division:
<http://www.ombudsman.mb.ca/phia.html>

■ **MANITOBA – FIPPA:**

- Manitoba Culture, Heritage and Tourism, Provincial Archives Access Services:
<http://www.gov.mb.ca/chc/fippa/index.html>
- Office of the Manitoba Ombudsman, Access and Privacy Division:
<http://www.ombudsman.mb.ca/fippa.html>

■ **CANADA:**

- Treasury Board of Canada Secretariat:
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.html
- Privacy Commissioner of Canada, news release on Treasury Board Canada's privacy impact assessment policy: http://www.privcom.gc.ca/media/nr-c/02_05_b_020424_e.asp

■ **ALBERTA:**

- Alberta Government Services, Information Management Access and Privacy Branch:
http://www3.gov.ab.ca/foip/guidelines_practices/2002/chapter9.cfm
- Office of the Information and Privacy Commissioner:
<http://www.oipc.ab.ca/pia/>

■ **BRITISH COLUMBIA:**

- British Columbia Ministry of Management Service, Corporate Privacy and Information Access Branch: http://www.msar.gov.bc.ca/foi_pop/manual/forms/pia.doc
- Office of the Information and Privacy Commissioner:
<http://www.oipcbc.org/public/pia/>

■ **ONTARIO:**

- Ontario Management Board Secretariat, Corporate Freedom of Information and Privacy Office: <http://www.gov.on.ca/MBS/english/fip/pia/>
- Office of the Information and Privacy Commissioner:
<http://www.ipc.on.ca/english/resources/resources.html>

IMPORTANT NOTE TO USERS:

PHIA and FIPPA are intricate statutes in themselves and also in their relationship to one another. While they are based on common principles of fair information practices, they have both obvious and subtle differences. We have tried to keep this Privacy Compliance Tool as generically based, short, and user friendly as possible. The purpose of the "Checklist" and "Guide" should be kept constantly in mind: to provide a step-by-step privacy compliance diagnostic process that covers the basic requirements of good information privacy practices.

The content of this Privacy Compliance Tool has been developed based on the understanding and experience of the authors with respect to compliance with PHIA and FIPPA, and government policy. It is not intended to provide legal advice. Users requiring legal advice are encouraged to consult counsel.

ELEMENT 1

IDENTIFYING PURPOSES AND LIMITING COLLECTION OF PERSONAL HEALTH INFORMATION

Collection of *personal health information* must be in accordance with the provisions of PHIA, and be limited to the purpose identified by the organization.

NOTE that *personal health information* "sharing" or "exchange" is not a concept defined in PHIA. If the collection of such information forms part of an *Information Sharing Agreement*, the agreement must comply with the provisions of the Act.

This Element requires that organizations:

Identify the Purpose for which *personal health information* is collected, either before it is collected or as soon as practicable afterward (under PHIA).

Limit Collection of *personal health information* to that which is necessary for the purposes identified by the organization.

Collect information directly from the individual unless *indirect collection* is authorized under the legislation.

Inform (notify) the individual when collecting directly of the purpose, and provide contact information for an official who can answer queries about collection.

What does the Law Say about Identifying the Purpose and Limiting the Amount of Information Collected?

PHIA restricts the collection of personal health information. A trustee shall not collect personal health information about an individual unless:

- (a) the information is collected for a lawful purpose connected with a function or activity of the trustee; and
- (b) the collection of the information is necessary for that purpose.

[Reference -- Section 13\(1\)](#)

A trustee shall collect only as much personal health information about an individual as is reasonably necessary to accomplish the purpose for which it is collected (section 13(2)).

What does the Law Say about Manner of Collection?

PHIA: Whenever possible, a trustee shall collect personal health information directly from the individual the information is about (section 14(1)) unless it falls within the five exceptions provided under the Act (section 14(2)).

What does the Law Say about Notification of Collection?

PHIA: A trustee who collects personal health information directly from the individual the information is about shall, before it is collected or as soon as practicable afterwards, take reasonable steps to inform the individual

- (a) of the purpose for which the information is being collected; and
- (b) if the trustee is not a health professional, how to contact an officer or employee of the trustee who can answer the individual's questions about the collection.

Reference -- Section 15(1)

A trustee need not comply with subsection 15(1) if the trustee has recently provided the individual with the information referred to in that subsection about the collection of the same or similar personal health information for the same or a related purpose (section 15(2)).

What does this Mean for your Organization?

Identifying the reason why an organization needs to collect *personal health information* is the first step in privacy compliance. If the collection of personal health information is not authorized, the organization should not be collecting it, so this is an important threshold question. An organization must be clear and “up front” about what information is collected, used, and disclosed in program activities. Failing to document the need for such information may result in additional administrative costs, including client or employee complaints, and make it difficult to track and manage the *personal health information* for which the organization is responsible.

Trustees are bound by PHIA requirements whether they collect *personal health information* or authorize an outside agent to collect information on their behalf (e.g. under contract).

The *collection* limitation principle constrains the amount and type of *personal health information* collected for an organization's activities. There must be an established link between the data collected and the purposes identified for collecting the information. Collecting more information than is needed may expose your organization to risk and to public scrutiny of privacy practices.

Personal health information is collected either directly (from the person the information is about) or indirectly (from another source). *Direct collection* is the preferred method of *collection*. *Indirect collection* should only be undertaken in limited circumstances, such as:

- where *direct collection* is difficult or impossible;
- where *direct collection* would result in inaccurate information; or,
- when law authorizes *indirect collection*.

When information is collected directly from clients/individuals, they should be informed about the *collection, use, and disclosure of personal health information*.

Recommended Best Practices

- ✓ Document the purpose for collecting *personal health information*, and make this information available to the public.

When considering PHIA with respect to a purpose of *collection, use, and disclosure of personal health information* under Part 3 of the Act, a *trustee* may find it useful to draw on a “reasonable person test” within the context of the preamble at the beginning of the legislation and its statement of purposes (section 2). This test,³ as articulated by the Office of the Privacy Commissioner of Canada in relation to the federal *Personal Information Protection and Electronic Documents Act*,

³ This is an adaptation of the “Oakes Test” from the Supreme Court of Canada case: *The Queen v. Oakes*, [1986] 1 S.C.R. 103 (see <http://www.lexum.umontreal.ca/>).

indicates that an entity may collect, use, and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances: the measure must be demonstrably necessary to meet some specific need; it must be demonstrably likely to be effective in achieving its intended purpose; the intrusion on privacy must be proportional to the benefit to be derived; and, it must be demonstrable that no other less privacy-intrusive measure would suffice to achieve the same purpose. Application of this test is not a requirement under PHIA.

- ✓ Contact your Privacy Officer for advice when you are planning a new program that involves the *collection of personal health information* or when revising existing *collection* practices.
- ✓ When defining what *personal health information* is necessary to meet operational or legislated requirements, consider both primary and secondary purposes (administration, quality improvement, program marketing, research, planning, etc.).
- ✓ Ensure employees or third parties collecting *personal health information* on your behalf understand what the rules are and can explain clearly the purpose of collection. They should know to whom they could refer people if there are any additional questions about the *collection of personal health information*.
- ✓ Limit the amount and type of *personal health information* collected to the amount necessary (i.e. “need to know” rather than “nice to know” or just “want to know”). Do not collect information for an unspecified purpose or “just in case” it might be useful at some future date.
- ✓ Be specific and avoid using broad purpose statements that could cause confusion or ambiguity.
- ✓ Prior to using “cookies” or any other process that collects identifiable information electronically provide notice of the practice or obtain consent.
- ✓ When designing *notification* processes, seek feedback from patients, clients, and employees, and engage front-line business personnel.

ELEMENT 2

LIMITING USE, DISCLOSURE, AND RETENTION OF PERSONAL HEALTH INFORMATION

In general terms, *personal health information* may be used or disclosed only for the purposes for which it was collected or with the *consent* of the individual or as authorized by law. Of paramount importance, it should be noted that PHIA emphasizes that every *use* and *disclosure* must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed.

Personal health information must be retained in accordance with a written retention and disposal policy that conforms to law and policy.

This Element in the “Checklist” deals with the disclosure of *personal health information* for health research under PHIA Section 24. Please refer to the introduction to the “Guide”, which provides additional important detail not repeated here about *information sharing agreements* and research.

NOTE that *personal health information* “sharing” or “exchange” is not a concept defined in PHIA. If the *disclosure* of such information forms part of an *Information Sharing Agreement*, the agreement must comply with the provisions of the Act.

The rules for this Element are contained in Part 3 of PHIA.

What does the Law Say about Use and Disclosure of Personal Health Information?

PHIA: Use of personal health information

A trustee shall not use or disclose personal health information except as authorized under this Division (section 20(1)).

Every use and disclosure by a trustee of personal health information must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed (section 20(2)).

A trustee shall limit the use and disclosure of personal information it maintains to those of its employees and agents who need to know the information to carry out the purpose for which the information was collected or received or to carry out a purpose authorized under section 21.

Restrictions on use of information: A trustee may use personal health information only for the purpose for which it was collected or received and shall not use it for any other purpose, unless:

- (a) the other purpose is directly related to the purpose for which the personal health information was collected or received;
- (b) the individual the personal health information is about has consented to the use;
- (c) Use of the information is necessary to prevent or lessen a serious and immediate threat to... an individual, or public health or public safety;
- (d) the trustee is a public body or health care facility and the personal health information is used:
 - (i) to deliver, monitor, or evaluate a program that relates to the provision of health care or payment for health care by the trustee; or
 - (ii) for research and planning that relates to the provision of health care or payment for health care by the trustee.
- (e) the purpose is one for which the information may be disclosed to the trustee under section 22; or
- (f) use of the information is authorized by an enactment of Manitoba or Canada.

[Reference -- Section 21](#)

NOTE: some sections have been excerpted or contracted here.

PHIA: Restrictions on disclosure of information:

Except as permitted by subsection (2), a trustee may disclose personal health information only if

- (a) the disclosure is to the individual the personal health information is about or his or her representative;
- (b) the individual the information is about has consented to the disclosure (section 22(1)).

Disclosure without individual's consent: A trustee may disclose personal health information without the consent of the individual the information is about if the disclosure is

- (a) to a person who is providing or has provided health care to the individual, to the extent necessary to provide health care to the individual, unless the individual has instructed the trustee not to make the disclosure;
- (b) to any personnel if the trustee reasonably believes that the disclosure is necessary to prevent or lessen a serious and immediate threat to an individual, or to public health or public safety;
- (c) For the purpose of
 - (i) contacting a relative or friend of an individual who is injured,
 - (ii) assisting in identifying a deceased individual, or
 - (iii) informing the representative or a relative of a deceased individual, or any other person it is reasonable to inform ..., of the individual's death;
- (d) to a relative of a deceased individual if the trustee reasonably believes that disclosure is not an unreasonable invasion of the deceased's privacy;
- (e) required for
 - (i) the purpose of peer review by health professionals,
 - (ii) the purpose of review by a standards committee,
 - (iii) the purpose of a body with statutory responsibilities for the discipline of health professionals..., or
 - (iv) the purpose of risk management assessment;
- (f) in accordance with section 23 (disclosure to the patient's family), 24 (disclosure for health research) or 25 (disclosure to an information manager);
- (g) for the purpose of... delivering, evaluating, or monitoring a program of the trustee that relates to the provision of health care or payment for health care, or... for research and planning that relates...;
- (h) to a computerized health information network and database, established by the government or another trustee that is a public body specified in the regulations, in which personal health information is recorded...;
- (i) to the government, another public body or the government of another jurisdiction... to the extent necessary to obtain payment for health care...;
- (j) to a person who requires the personal health information to carry out an audit for or provide legal services to a trustee...;
- (k) required in anticipation of or for use in a civil or quasi-judicial proceeding to which the trustee is a party, or the prosecution of an offence;
- (l) required to comply with a subpoena, warrant, or order issued or made by a court...;
- (m) for the purpose of
 - (i) an investigation under or the enforcement of an enactment of Manitoba..., or
 - (ii) an investigation or enforcement respecting a fraud related to the payment for health care;
- (n) for the purpose of complying with an arrangement or agreement entered into under an enactment of Manitoba or Canada; or
- (o) authorized or required by an enactment of Manitoba or Canada.

[Reference -- Section 22\(2\)](#)

NOTE: some sections have been excerpted or contracted here.

What does the Law Say about Retention of Personal Health Information?

PHIA: A trustee shall establish a written policy concerning the retention and destruction of *personal health information* and shall comply with that policy (section 17(1)).

What does this Mean for your Organization?

The general duty of trustees is to not use or disclose *personal health information* except in accordance with the legislation.

Limiting Use

A trustee's use of *personal health information* must be limited to the amount necessary to carry out the identified purpose of its collection. For example, an employee in a particular department who needs access to *personal health information* in a database should be provided access only to those data elements needed to do his or her job. *Personal health information* may be used for another purpose directly related to the purpose for which the information was collected or received (section 21, 21(a)).

An individual's *consent* should be obtained prior to using his or her *personal health information* for any additional purpose.

Limiting Disclosure

Again, broadly speaking, an organization may not disclose (i.e. share with a third party) *personal health information* unless that *disclosure* is consented to by the individual or authorized by legislation. *Disclosure* of *personal health information* should be limited to only that information necessary to achieve the intended purpose. *Disclosure* is generally not compulsory. In most cases, organizations may exercise discretion as to whether or not to disclose information under one of the circumstances framed in the legislation.

Consent should be the starting point when staff considers possible *disclosure* of *personal health information*. This does not mean that you must obtain *consent* in all circumstances. The Act recognizes various legal requirements and operational situations when obtaining *consent* may not be necessary or reasonably possible. A number of regulatory bodies, such as The College of Physicians and Surgeons of Manitoba, have by-laws and guidelines that may assist particular types of trustees in drafting a records retention and destruction policy.

Limiting Retention

PHIA requires a written records retention and destruction policy with respect to *personal health information*.

Recommended Best Practices

- ✓ Consider the reasonable expectations of individuals when determining the method of obtaining *consent*.
- ✓ Consider meaningful *consent* the starting point for disclosure of *personal health information*.
- ✓ *Consent* forms should include at least the following:⁴
 - A clear description of the information to be used or disclosed,
 - The date the consent is effective and when it expires (avoid open-ended consents),
 - The name of the organization authorized to use or receive the information,
 - The purpose for the *use* or *disclosure*, and
 - The signature of the individual (or his/her *authorized representative*).

⁴ In the absence of detailed statutory rules, the Ombudsman's Office has prepared a one-page "Elements of Consent for Personal Health Information under PHIA" (see *Appendix 2* of this "Guide").

- ✓ Use and disclose the least amount of information possible to achieve the required purpose.
- ✓ When considering PHIA with respect to *collection, use, and disclosure of personal health information* under Part 3 of the Act, a *trustee* may find it useful to draw on a “reasonable person test” within the context of the preamble at the beginning of the legislation and its statement of purposes (s.2). For further detail on this test, see Element 1 above under the first entry within “Recommended Best Practices”.
- ✓ Use and disclose de-identified information whenever possible for policy planning, research or statistical purposes.
- ✓ Use administrative, physical, and technical controls to limit access to *personal health information* to staff members and contractors who have a “need to know”.
- ✓ Consider this “need to know” as a design principle to regulate access when developing new computer systems that contain *personal health information*.
- ✓ Staff should maintain a complete audit trail of what *personal health information* has been disclosed (e.g. for what purpose, to whom, and under what authority).
- ✓ Contents of *Information Sharing Agreements*. Consultation with legal counsel is advisable, but some core considerations are likely to be:
 - the purpose(s) of the agreement,
 - the legal or other authority for information sharing and on which the agreement relies,
 - the purpose(s) for which the information is being used by the entity to which it is disclosed,
 - a description of the *personal health information* to be shared/disclosed and what information will be matched/linked/shared, and any limitations on subsequent uses and disclosures,
 - identification of the administrative, technical, and physical safeguards required to protect the *confidentiality* of the information,
 - a clause that allows the information provider(s) to access the premises of the other party to ensure that it is abiding by the agreement,
 - provisions for compliance auditing,
 - mechanisms for amending and resolving disagreements over the terms of the agreement,
 - duration of the agreement,
 - sanctions for non-compliance, such as termination of the contract, and
 - disposition of the information.

ELEMENT 3

ENSURING ACCURACY OF PERSONAL HEALTH INFORMATION

Personal and personal health information collected must be as accurate, complete, and up-to-date as necessary for the purposes for which they are to be used.

What does the Law Say about Accuracy?

PHIA: Before using or disclosing personal health information, a trustee shall take reasonable steps to ensure that the information is accurate, up to date, complete, and not misleading (section 16).

For the purposes of accuracy or completeness, an individual may request a trustee to correct any personal health information that the individual may examine and copy under this Part (section 12(1)).

Note: the timelines and detailed process for correction requests are contained in sections 12(2) to 12(6).

What does the Law Say about Notice to Others about Correcting a Record?

PHIA: When a trustee makes a correction or adds a statement of disagreement under this section, the trustee shall, when practicable, notify any other trustee or person to whom the personal health information has been disclosed during the year before the correction was requested about the correction or statement of disagreement. A trustee who receives such a notice shall make the correction or add the statement of disagreement to any record of that personal health information that the trustee maintains (Section 12(5)).

What does this Mean for your Organization?

The purpose of the accuracy principle is to minimize the possibility that a decision affecting an individual will be made on the basis of inaccurate or outdated *personal health information*. Organizations must make reasonable efforts to ensure that information used to make a decision that directly affects the individual is accurate and complete. This process involves careful verification of *personal health information* when it is collected and/or entered into a database.

The purposes for which you collect, use, and disclose *personal health information* will determine how often it must be checked for accuracy. Normally, you only need to update previously collected *personal health information* if it is required for ongoing provision of services, or if the individual concerned asks you to do so. It is good practice to update personal information at point of direct contact with the specific individuals.

The statute enables individuals to request a correction of their *personal health information*. When there is a refusal to make a correction by a *trustee*, PHIA requires the applicant be notified of the reason for the decision and of his or her right to complain to the Ombudsman. PHIA specifies that the individual whose request for a correction has been refused must be informed of his or her right to add a concise statement of disagreement to the record. The Act also contains provisions for notifying others to whom the information has been disclosed during the year preceding the request for correction. These provisions should be consulted directly (PHIA section 12(5))

Recommended Best Practices

- ✓ Implement processes to modify or correct hard copy or electronic files containing *personal health information*.
- ✓ Document when the file was last compiled or updated, and by whom.
- ✓ If a correction is made, make reasonable efforts to ensure that all other records that contain the same *personal health information* are also updated.
- ✓ Conduct periodic assessments of accuracy in your databases (for example, when an individual seeks services).
- ✓ Notify others who have received inaccurate information of the requirement to correct the data.

ELEMENT 4

SAFEGUARDING PERSONAL HEALTH INFORMATION

Organizations are required to protect *personal health information* by making reasonable security arrangements against risks such as unauthorized access, *use*, *disclosure* or destruction/obliteration. These security requirements apply to records in hard copy form as well as to records that are kept electronically such as a database. While the general security requirements for hard copy and electronic records are the same, the implementation of safeguards will be specific to the information medium.

Note that *The Personal Health Information Regulation 245/97*, in addition to the sections noted below, deals with establishing what *personal health information* may be accessed by agents and employees of trustees, orientation and training, a pledge of confidentiality, and auditing security safeguards at least every two years.

What does the Law Say about Safeguarding Information?

PHIA: A trustee shall establish a written policy concerning the retention and destruction of personal health information and shall comply with that policy (section 17(1)).

A policy under section 17(1) must conform to any requirements of the regulations (section 17(2)).

In accordance with any requirements of the regulations, a trustee shall ensure that personal health information is destroyed in a manner that protects the privacy of the individual the information is about (section 17(3)).

In accordance with any requirements of the Regulations, a trustee shall protect personal health information by adopting reasonable administrative, technical, and physical safeguards that ensure the confidentiality, security, accuracy, and integrity of the information (section 18(1)).

Without limiting section 18(1) a trustee shall

- (a) implement controls that limit the persons who may use personal health information maintained by the trustee to those specifically authorized by the trustee to do so;
- (b) implement controls to ensure that personal health information maintained by the trustee cannot be used unless
 - (i) the identity of the person seeking to use the information is verified as a person the trustee has authorized to use it, and
 - (ii) the proposed use is verified as being authorized under this Act;
- (c) if the trustee uses electronic means to request disclosure of personal health information or to respond to requests for disclosure, implement procedures to prevent the interception of the information by unauthorized persons; and
- (d) when responding to requests for disclosure of personal health information, ensure that the request contains sufficient detail to uniquely identify the individual the information is about.

[Reference -- Section 18\(2\)](#)

A trustee who maintains personal health information in electronic form shall implement any additional safeguards for such information required by the regulations (section 18(3)).

In determining the reasonableness of security safeguards required under Section 18, a trustee shall take into account the degree of sensitivity of the personal health information to be protected (section 19).

PHIA Regulations:

A trustee shall establish and comply with a written policy and procedures containing the following:

- (a) provisions for the security of personal health information during its collection, use, disclosure, storage and destruction, including measures
 - (i) to ensure the security of the personal health information when a record of the information is removed from a secure designated area, and
 - (ii) to ensure the security of personal health information in electronic form when the computer hardware or removable electronic storage media on which it has been recorded is being disposed of or used for another purpose.
- (b) provisions for the recording of security breaches;
- (c) corrective procedures to address security breaches.

[Reference -- Reg 245/97, section 2](#)

Access restrictions and other precautions: A trustee shall

- (a) ensure that personal health information is maintained in a designated area or areas and is subject to appropriate security safeguards;
- (b) limit physical access to designated areas containing personal health information to authorized persons;
- (c) take reasonable precautions to protect personal health information from fire, theft, vandalism, deterioration, accidental destruction or loss, and other hazards; and
- (d) ensure that removable media used to record personal health information is stored securely when not in use.

[Reference -- Reg. 245/97, section 3](#)

Additional safeguards for electronic health information systems

- 4(1) A trustee shall ensure every electronic information system that the trustee designs or acquires after December 11, 2000
 - (a) produces an electronic record of every successful or unsuccessful attempt to (i) gain access to the personal health information maintained on the system, (ii) add to, delete or modify the personal health information maintained on the system; and
 - (b) records every transmission of personal health information maintained on the system.
- 4(2) A trustee shall regularly review the electronic records produced under subsection (1) to detect any security breaches.
- 4(3) The requirements of this section only apply to an electronic information system used by a trustee to maintain personal health information.

[Reference -- Reg. 245/97, section 4](#)

What does this Mean for your Organization?

Protecting *personal health information* from unauthorized access requires the implementation of administrative, physical, and technical safeguards. These measures are necessary to ensure that sensitive information is not compromised in any respect. The assessment of security safeguards must include the evaluation of threats from within and outside the organization. Studies have documented time and again that the “insider” threat to the security of information is at least equal to and usually greater than that posed by “outsiders”. Further, research has shown that organizations tend to pay less attention to or even virtually ignore the internal threats to information security!

The measures used to safeguard information should be appropriate to the sensitivity and magnitude of the *personal health information* involved, bearing in mind that “sensitivity” carries a degree of subjectivity for individuals in the context of their particular circumstances. Some types of *personal health information* are generally thought to be more sensitive than others. Socio-economic factors have a significant influence on what information an individual considers most sensitive. The assessment of information sensitivity must take account of the context of the information. The level of sensitivity -- and, therefore, the level of safeguards -- may be analysed by assessing the potential harm or other adverse affect to the individual if the information were released to unauthorized parties.

Recommended Best Practices

Analyze the type and characteristics of *personal health information* in your custody and control, the varying levels of sensitivity for each type of information, and the risks that may pertain to it.

- ✓ Examples of administrative, physical, and technical safeguards are:
 - security policies and procedures,
 - training and awareness programs,
 - background checks for new employees, and a pledge of confidentiality,
 - use of physical barriers, security areas, and access and authorization mechanisms to restrict access,
 - use of software, hardware, or operating system access and audit controls,
 - security requirements stipulated in contracts with third parties,
 - information sharing agreements with those to whom you disclose information on a regular basis,
 - use of secure communications for transmission of sensitive information,
 - manual dispatch of sensitive information rather than fax or electronic transmission. If you are sending information electronically, assess the security features of the networking environment and address potential vulnerabilities of the network to hacking or inappropriate access by third parties.

- ✓ Examples of information-handling practices:
 - ensure the security and protection of the information from collection through to final disposition,
 - secure personal health information when leaving your desk,
 - ensure fax machines are in a secure, non-public area,
 - when sending a fax, confirm the fax number and ensure someone is waiting to receive the information,
 - use a cover sheet and include a confidentiality statement on fax and e-mail transmissions,
 - encrypt e-mails containing sensitive personal health information,
 - protect the security and integrity of personal health information under your control through the use of security passwords at your workstation, and change them regularly,
 - find out how long records containing personal health information must be kept and whether or not you are authorized to destroy or delete them.

ELEMENT 5

ENSURING INDIVIDUAL ACCESS TO PERSONAL HEALTH INFORMATION

An individual or his/her *authorized representative* is entitled to have access to *personal health information* and to information concerning the *personal health information* an organization holds about him or her.

A *trustee* has the duty to assist an individual making an application or request for access to his or her *personal health information*.

What does the Law Say about Individual Access?

PHIA: Right to examine and copy information

Subject to this Act, an individual has a right, on request, to examine and receive a copy of his or her personal health information maintained by a trustee (Section 5(1)).

Note: basic detail regarding access requests for personal health information is contained in Sections 5 to 12 of PHIA.

WHAT DOES THIS MEAN FOR YOUR ORGANIZATION?

Under PHIA, individuals have a right of access to information about themselves in the custody or under the control of a *trustee*, subject only to limited and specific exceptions. Individuals can make a formal request to access their personal file or any information that you may hold about them. Access may also be provided “outside” the legislation so long as the “informal” procedures do not circumvent the individual’s access rights or compromise a third party’s privacy rights. The formal procedures under PHIA are not intended to be invoked automatically, but more as a measure of last resort for access to one’s own *personal health information*.

It may not always be possible to release all information held about an individual. Nevertheless, access refusals must be reasonable, limited, and justified. If individuals are refused access to their information, an organization must provide an explanation for the refusal. There are very limited grounds for such refusal.

The Act stipulates that every reasonable effort must be made to assist an individual and to respond without delay, openly, accurately, and completely.

RECOMMENDED BEST PRACTICES

- ✓ Establish an informal process for dealing with routine, simple requests by individuals (e.g. a patient asks her physician for the results of her lab test). Implement a formal process for requests that are unusual, involve severing of information, or require extensive use of internal resources.
- ✓ Ensure all formal requests and responses are in writing, but note that PHIA does not require a written request, although it allows a trustee to require a request in writing.
- ✓ Implement methods of authenticating the identity of the individual.
- ✓ Implement methods of verifying the rights of an *authorized representative* to act on another’s behalf.
- ✓ Establish procedures to ensure that the individual receives only his or her own *personal health information*, not the information of third parties.

ELEMENT 6

CHALLENGING COMPLIANCE

People have the right to question a *trustee* about compliance with the personal health information privacy protection provisions under PHIA. Parts 4 and 5 of PHIA provide the Manitoba Ombudsman with broad powers, duties, and responsibilities for overseeing compliance with the legislation. The Ombudsman reports annually to the Legislature and may, in the public interest, publish a special report on any matter within the scope of the powers and duties of the Act on any particular matter investigated. The Ombudsman investigates and reports on complaints, and may also initiate an investigation or review any matter respecting the Act where there are reasonable grounds to do so.

Respecting *personal health information*, an individual may complain under PHIA if, for example, an individual feels that a trustee:

- has not responded to a request for access within the time limits set out in the Act,
- has refused access to an individual's own recorded *personal health information*,
- has charged an unreasonable or unauthorized fee related to an access request,
- has refused to correct an individual's own *personal health information*,
- has collected, used or disclosed *personal health information* about an individual that is believed to be contrary to his/her information privacy rights or to what the legislation may permit.

Individuals who believe their information access or privacy rights have been breached may be directed to contact the Ombudsman's Office by mail, phone, fax, or in person. They will be asked to provide a written complaint to the Office or will be assisted if the individual has difficulty putting the complaint in writing. Complaints under PHIA must be in writing, describing the concerns. Investigations and reviews are conducted in private and as informally as possible. Nevertheless, the Ombudsman may exercise the legislated power under *The Manitoba Evidence Act* to summon witnesses and to take evidence under oath. On completion of an investigation, the complainant and the *trustee* will be provided with a report on the findings of the Office. A *trustee* must respond to any recommendations in the report. If a recommendation is not accepted, further action may be taken including the Ombudsman reporting publicly or, in the case of recommended release, an appeal to the Court of Queen's Bench.

It is extremely important that the public's right to bring complaints about alleged infractions of the legislation is made known routinely and on a timely basis to individuals. The right to challenge compliance is one of the fundamental tenets of internationally accepted principles of fair information practices.

ELEMENT 7

ACCOUNTABILITY AND OPENNESS OF POLICIES AND PRACTICES

An organization is responsible for personal health information in its custody or under its control and specific individual(s) are designated by law and policy to be accountable for the organization's compliance with established privacy principles.

An organization must make information relating to the management of personal health information available to the public.

What does the Law Say about Accountability and Openness?

PHIA: "Trustee" means a health professional, health care facility, public body, or health services agency that collects or maintains personal health information (section 1).

A health care facility and a health services agency shall designate one or more of its employees as a privacy officer whose responsibilities include

- (a) dealing with requests from individuals who wish to examine and copy or to correct personal health information under the Act; and
- (b) generally facilitating the trustee's compliance with this Act.

[Reference -- Section 57](#)

Where a trustee is a public body, any decision made or opinion formed under this Act by the trustee may be made or formed by the head of the public body as defined in *The Freedom of Information and Protection of Privacy Act* (section 58(1)).

What does this Mean for your Organization?

Operational and coordinating responsibilities for the lawful *collection, use, disclosure*, retention, and security of *personal health information* must be specifically assigned within an organization. These responsibilities also encompass internal policies and procedures that need to be in place to facilitate the integration of privacy protection practices into the organization at all levels and to monitor compliance. The roles and responsibilities of various individuals should be clearly identified in the organization's structure, and should include:

- identification of risks,
- assessment of data management practices,
- administration of privacy breaches,
- effective implementation of policies and procedures, and
- ongoing monitoring of privacy best practices.

Organizations remain accountable for *personal health information* that is provided to contractors to conduct services on their behalf. Examples may include:

- a provider of information and records management or technology services,
- an outsourced payroll service,
- a contracted data collector,
- a contractor who "teleworks".

Among the major risks to privacy are the data-handling practices of third parties who may not be aware of their clients' stringent privacy and security requirements. Organizations are responsible for making third parties aware of applicable law, privacy policies and requirements, and for monitoring compliance with their established privacy standards.

Knowledge of an organization's privacy policies and practices allows individuals to make informed choices before revealing *personal health information*. Members of the public should have the opportunity to assess whether an organization's privacy practices meet their own expectations of privacy and *confidentiality*.

Where they may exist, internal complaint review processes relating to *personal health information* should not interfere in any way with an individual's right to complain to the Office of the Ombudsman.

Recommended Best Practices

- ✓ Publish the title and phone number of a person within your organization who can provide privacy advice or handle complaints.
- ✓ Establish contracts requiring third parties to comply with privacy and security standards.
- ✓ Give front-line staff specific instructions on *disclosure of personal health information*, requests for access, and how to manage or re-direct an access or privacy complaint.
- ✓ Include privacy, *confidentiality*, and security training in orientation programs for new employees and contractors.
- ✓ Make information management and information privacy policies and practices available through brochures, web sites, or telephone recordings.
- ✓ Inform your employees that web browsing and e-mail may be monitored where this is the case. Such monitoring should always be necessary and reasonable under the circumstances.
- ✓ Consider communicating the organization's compliance with privacy policies by making privacy impact assessments available to the public except for parts that may compromise security.
- ✓ Consider developing a Privacy Charter or privacy policy statement as a general declaration of an organization's practice in relation to *collection, use, and disclosure of personal health information* about individuals. This general policy should include details about:
 - **Accuracy** – measures adopted to ensure accuracy of *personal health information* collected,
 - **Security** – measures adopted to ensure security and confidentiality of the information;
 - **Access and correction** – how an individual can request access to or request a correction of *personal health information* held about him or her;
 - **Disclosure** – the circumstances under which *personal health information* is transferred to third parties;
 - **Complaints process** – how complaints are handled within the organization.
- ✓ Publicize how patients, clients and employees may file a complaint concerning information privacy practices including such avenues as professional bodies in addition to the Ombudsman's Office.

ELEMENT 8

ASSESSING PRIVACY RISKS IN ELECTRONIC SERVICE DELIVERY (ESD)

Public and private sector organizations are under sustained pressure to implement convenient, rapid, effective, and efficient delivery of services to the public. The bundling of services to meet these growing demands through the sharing of *personal health information* across programs using a common delivery infrastructure can be challenging, but enhanced service delivery should and can still assure appropriate levels of privacy protection, including security. Projects involving the electronic delivery of services must be carefully examined for the way in which processes and data flows are integrated, and the manner in which access is managed. It bears repeating here that organizations remain accountable for *personal health information* that is provided to contractors or other third parties to conduct services on their behalf.

It should always be borne in mind that the privacy provisions of PHIA are intended to protect *personal health information*. Early incorporation of the letter and spirit of the law into the activities, programs, and the very culture of organizations is important to avoid breaches of privacy, which as a rule cannot be undone or adequately remedied. Where new programs or legislative schemes are being contemplated, privacy protection should be a routine part of the planning and design processes. Privacy “retrofits” are rarely easy, inexpensive, or as fully effective as a properly planned initiative. They are never the approach of choice.

The Privacy Compliance “Checklist” for Electronic Service Delivery, Element 8, is designed to help avoid common pitfalls of ESD implementation, including:

- failure to consider the requirements of applicable privacy legislation and fair information practices,
- failure to consider relevant policies or procedures related to privacy and security,
- inadequate control over the actions of service providers,
- underestimating the impact to privacy of specific technology or design choices (such as Public Key Infrastructure or biometrics),
- improper analyses of data flows and data linkages,
- inadequate consideration of stakeholder reaction, including the public’s, and
- insufficient user awareness and training for authorized users about the organization’s security and privacy policies.

Elements 1-7 of the Privacy Compliance “Checklist” should be used as guiding principles for ESD project teams to use during the earliest stages of systems design. They must be the overarching principles that guide the analysis of the fit between data elements, business process, and technical design choices. Demonstrating compliance with the first seven “Checklist” elements can be performed at early stages of systems development in a standard development lifecycle, such as at the concept or definition phase.

The “Checklist” includes questions that focus attention on some of the critical risks to privacy of ESD initiatives. Some of these risks are associated with the technical design and architecture of the system while others relate to the functioning of the program or public service.

Individual Profiling and Monitoring

To be effective, some programs may need to link previously unrelated stores of *personal health information* to create new information about an identifiable individual. Data linking can be conducted through centralized storage of personal information or by linking and matching personal data from separate databases.

The purpose of many ESD proposals is the cost-effective delivery of multiple services requiring similar information. Where previously separate services are bundled, *personal health information* may be collected at a single point and accessed in a distributed program environment. Single point-of-entry

services often require unique or common identifiers across systems, both of which are likely to have an impact on individual privacy.

In order to provide ongoing improvements in the nature and delivery of services, some programs may monitor transactions. Such monitoring generates additional personal information about individuals' interactions with systems and may reflect user preferences with respect to specific programs and services. Current surveys and studies show clearly that the public is very concerned about the monitoring of online activities and transactions. ESD project teams should prudently gauge and preferably test public reaction prior to developing and implementing electronically assisted services.

Method of Service Delivery

Alternative methods of service provision are a means by which organizations may leverage effective systems and distribution infrastructures to increase effectiveness and reduce cost. Partnerships between the public and private sector to deliver public services often present new circumstances to consider. Whereas members of the public may exercise choice in their interactions with the private sector, their interactions with government offer less discretion and are frequently more intimate and complicated.

Individuals are often required to provide sensitive *personal health information* to establish eligibility for government programs and services. Where such delivery of services is outsourced to the private sector, concerns about privacy are usually increased. Organizations subject to PHIA must ensure that organizational accountability and compliance oversight extends to contractors and sub-contractors.

The choice of delivery channel can also pose risks to privacy. Where previously separate services are bundled and offered through common channels such as kiosks or call centers, complex issues of identification and authentication may emerge.

System Design and Characteristics

Systems design and technology choices must be made carefully with reference to the relationships between privacy and security. Technology choices should be evaluated for their ability to enhance privacy. Even privacy-enhancing technologies often have their own privacy-invasive characteristics, and these should be acknowledged, analyzed, and managed in a privacy protective manner. Where access management is based on common directory services, it is important to ensure that the association between individuals and their service privileges is protected. Data matching and data linking or profiling frequently pose a threat where directory services support multiple programs.

The monitoring of ESD systems to analyze customer uses and preferences can also pose a risk to privacy. Transaction logging systems and the use of cookies should be implemented in a way that promotes the use of non-identifiable or aggregate data collection and analysis.

Recommended Best Practices

- ✓ Start the assessment process before or at least early in the electronic systems development lifecycle.
- ✓ Recognize that the "human element" represents the largest single threat to information security and have an ongoing and regularly updated awareness and training plan in place.
- ✓ Survey how similar options for electronic delivery of services have been handled in other jurisdictions. Examine how similar risks to privacy were mitigated. Undertaking an early analysis of project risks and mitigation factors will provide a timely perspective on the prevailing privacy landscape and place studies of ESD projects in other jurisdictions in context.
- ✓ When choosing alternate delivery methods for previously available public information, ensure that the increased ability to access, manipulate, and use such information does not present significant risks to privacy, is not likely to harm the individuals the information is about, and that the benefits to be gained are clearly in the public interest.

- ✓ Ensure compliance of service providers and other third parties through the use of contractual provisions and proactive audits. This could include an independent review by a trusted third party or by consulting with an oversight body for compliance with privacy rules.
- ✓ Weigh the options and find a reasonable, principled, and lawful balance between the sensitivity of the personal data to be processed by the system and the method of service delivery.
- ✓ Determine whether the true identity of the individual must really be known, or whether *anonymity* or pseudonymity or other privacy-enhancing techniques or technologies could be employed.
- ✓ Use methods such as data stripping or conversion of identifiers to promote the highest degree of *anonymity* in the analysis of data.
- ✓ Consider employing the minimum level of authentication required to ensure effective delivery of service. Choose privacy-enhancing, as opposed to privacy-invasive methods of authentication.
- ✓ Wherever possible, present members of the public with options for choosing the method of service delivery that suits their privacy preferences. For example, some individuals may choose to obtain common services through a portal while others may prefer interaction with call-center or other personnel.

APPENDIX 1

COMMON TERMS AND DEFINITIONS

The following are definitions of terms used in the Privacy Compliance “Guide” and “Checklist”. If the terms are defined in Part 1 of FIPPA or PHIA, that definition has been used. Terms defined in the legislation are identified below with an asterisk (*). The other definitions given are not legal definitions, but are intended to contribute to a general understanding of the concepts.

Anonymity:

Information is “anonymous” if the person the information is about cannot be identified. Information can be fully identifiable, fully anonymous or fall somewhere between those two extremes depending on how much information is provided, and the context of the information. Anonymization is the process of removing identifiers from personal health information so that specific individuals are not known.

Authorized representative:

In PHIA, certain persons may exercise the rights of an individual (or “stand in their shoes”).

The rights of an individual under PHIA may be exercised

- (a) by any person with written authorization from the individual to act on the individual’s behalf;
- (b) by a proxy appointed by the individual under *The Health Care Directives Act*;
- (c) by a committee appointed for the individual under *The Mental Health Act* if the committee has the power to make health care decisions on the individual’s behalf;
- (d) by a substitute decision maker for personal care appointed for the individual under *The Vulnerable Persons Living with a Mental Disability Act* if the exercise of the right relates to the powers and duties of the substitute decision maker;
- (e) by the parent or guardian of an individual who is a minor, if the minor does not have the capacity to make health care decisions; or
- (f) if the individual is deceased, by his or her personal representative.

[Reference -- Section 60](#)

Collection:

Collection occurs when staff or their agents assemble, accumulate, or gather personal health information in any form by any means including surveys, interviews, hard copy or electronic forms.

Confidentiality:

The act or duty of restricting access to information to those who are authorized and have a “need to know”.

Consent:

Permission from an individual or his or her *authorized representative* to use or disclose his or her own *personal health information*. See Appendix 2 for the “Elements of Consent for Personal Health Information under PHIA” prepared by the Ombudsman’s Office.

Data Linking:

Also referred to as “data profiling”. Refers to the computerized use of personal information received from an entity in another jurisdiction to merge and compare files on identifiable individuals or categories of individuals for administrative or operational purposes. This linkage or profiling activity generates a new body of *personal health information*. This activity could also occur within, between or among entities in the same jurisdiction.

Data Matching:

Generally means a comparison of a database(s) or set(s) of records of personal information held by an entity in one jurisdiction with another database(s) or set(s) of records of an entity in another jurisdiction and where the computer matching program creates or merges files on identifiable individuals to identify matters of interest or to generate additional information about the individuals to whom the *personal health information* relates. In some jurisdictions, certain data matching activities require special approval processes. This activity could also occur within, between or among entities in the same jurisdiction.

Direct Collection:

Collecting *personal health information* from the individual the information is about.

Disclosure:

Revealing *personal health information* outside the bounds of the trustee. This includes sharing information with individuals, friends, or family members of the individual.

Indirect Collection:

Collecting *personal health information* from sources other than the individual the information is about.

Information Manager*:

- (a) processes, stores or destroys personal health information for a trustee, or
- (b) provides information management or information technology services to a trustee.

Information Sharing Agreement:

May also be called a *personal health information* “Data Sharing Agreement”, among other things. Exchanging, collecting or disclosing *personal health information* by a party in one jurisdiction with a party in another jurisdiction for certain purposes. Data sharing may be carried out by using any transmission method, and may take place over any time period. The activities covered could also occur within, between or among entities in the same jurisdiction. Such activities within an organization would be considered a use (see definition below).

Local Public Body*:

- (a) an educational body,
- (b) a health care body, and
- (c) a local government body.

[Reference – FIPPA Section 1](#)

Notification or Notice:

The process of providing individuals with information about the collection of their *personal health information* when it is collected directly from individuals.

Personal Health Information*:

Recorded information about an identifiable individual that relates to

- (a) the individual's health, or health care history, including genetic information about the individual,
- (b) the provision of health care to the individual, or
- (c) payment for health care provided to the individual' and includes
- (d) the PHIN [Personal Health Identification Number as defined in *The Personal Health Information Act*] 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.

[Reference – PHIA Section 1](#)

Personal Information*:

Recorded information about an identified individual, including

- (a) the individual's name,
- (b) the individual's home address, or home telephone, facsimile or e-mail number,
- (c) information about the individual's age, sex, sexual orientation, marital or family status,
- (d) information about the individual's ancestry, race, color, nationality, or national or ethnic origin,
- (e) information about the individual's religion or creed, or religious belief, association or activity,
- (f) personal health information about the individual,
- (g) the individual's blood type, fingerprints, or other hereditary characteristics,
- (h) information about the individual's political belief, association, or activity,
- (i) information about the individual's education, employment or occupation, or educational, employment or occupational history,
- (j) information about the individual's source of income or financial circumstances, activities, or history,
- (k) information about the individual's criminal history, including regulatory offences,
- (l) the individual's own personal views or opinions, except if they are about another person,
- (m) the views or opinions expressed about the individual by another person, and
- (n) an identifying number, symbol, or other particular assigned to the individual.

[Reference – FIPPA Section 1](#)

Public Body*:

Public Body means

- (a) a department.
- (b) a government agency
- (c) the Executive Council Office,
- (d) the office of a minister, and
- (e) a local public body, but does not include
- (f) the office of a Member of the Legislative Assembly who is not a minister,
- (g) the office of an officer of the Legislative Assembly, or
- (h) the Court of Appeal, the Court of Queen's Bench or the Provincial Court.

[Reference – FIPPA Section 1](#)

Trustee*:

A health professional, health care facility, *public body* or health services agency that collects or maintains *personal health information*.

[Reference – PHIA Section 1](#)

Use:

The use and sharing of *personal health information* within the organization to accomplish the organization's purposes. Access to a file or database by program staff or contractors on a "need-to-know" basis would be considered a use under the Act. Use does not include disclosure.

APPENDIX 2

ELEMENTS OF CONSENT FOR PERSONAL HEALTH INFORMATION UNDER PHIA:

In offering the following elements of consent that should be addressed by a trustee of recorded personal health information about an identifiable individual, the Ombudsman's Office is not suggesting that there is a single consent form, activity or process by which informed consent may be obtained in the use or disclosure of personal health information.

Personal health information may only be collected, used or disclosed for purposes authorized under *The Personal Health Information Act*. Note that obtaining consent may not be employed as a means of collecting personal health information not otherwise authorized under the Act. There is no provision for consent in relation to the collection of personal health information from the individual the information is about, but this process is available for use and disclosure of personal health information lawfully collected. PHIA provides for the collection of personal health information from other sources in a limited number of circumstances, including when authorized by the individual.

Notwithstanding this, the limitation principle applies to the collection of personal health information as well as to its use and disclosure. In other words, every collection, use and disclosure must be limited to the minimum amount of personal health information necessary to meet the authorized purpose.

It is the duty of trustees to ensure that consent is obtained in a manner that is consistent with legislative provisions under *The Personal Health Information Act*. Under the legislation, consent may be required whenever personal health information is used by or disclosed to someone other than the individual the information is about.

We have put forward generic elements that could, in our opinion, be addressed in a flexible, reasonable, and effective manner so long as the process follows the law and the result is meaningful consent where it is required or sought. Addressing each of the elements of consent can contribute to ensuring that the trustee is providing the minimum amount of information through clear, specific and informed consent.

To ensure that the trustee will use and disclose the minimum amount of personal health information necessary to accomplish its purpose, the consent should be in writing and should address the following elements of consent:

- (a) the specific personal health information to be used or disclosed;
- (b) the identity of the person, organization or trustee that the personal health information may be used by or disclosed to;
- (c) all the purposes for the use or disclosure;
- (d) statement a from the trustee:
 - affirming that a third-party recipient will be instructed not to use or disclose the personal health information provided by the trustee, except for a purpose specified in the consent, and
 - specifying the subsequent disclosures, if any, that a third-party recipient will be instructed it is permitted to make;
- (e) an acknowledgement that the consenting individual has been made aware of:
 - why the personal health information is needed, and
 - the risks and benefits to the individual of consenting or refusing to consent to the use or disclosure;
- (f) the date the consent is effective, and the date the consent expires;
- (g) a statement that the consent may be revoked or amended at any time.

To make our suggestion clear, we reiterate our opinion that a consent form need not articulate every one of these elements under all circumstances, but each of the components should have been carefully considered in the process of preparing such a form. While it is not our role to prescribe or approve a specific form in advance of its use, we would be pleased to discuss the suggested elements with you.

[July 2003]