Chapter 6

TABLE OF CONTENTS

TABLE OF CONTENTS **1**

PROTECTION OF PRIVACY **7**

Overview **7**

Preliminary Privacy Considerations – Necessary, Effective and Proportional **11**

The Ombudsman's three part test 11
The Privacy Commissioner of Canada has developed a very similar 4 point test 12

The Privacy Principles in FIPPA **13**

PRINCIPLE #1: CONSENT 14
PRINCIPLE #2: ACCOUNTABILITY 14
PRINCIPLE #3: IDENTIFYING PURPOSES 15
PRINCIPLE #4: COLLECTION LIMITATION 16
PRINCIPLE #5: USE, RETENTION AND DISCLOSURE LIMITATION 17
Limits on Use 17
Limits on Retention 18
Limits on Disclosure 18
PRINCIPLE #6: ACCURACY 19
PRINCIPLE #7: SECURITY – SAFEGUARDING PERSONAL INFORMATION 19
PRINCIPLE #8: OPENNESS 20
PRINCIPLE #9: ACCESS TO AND CORRECTING ONE'S OWN PERSONAL INFORMATION 21
Access 21
Correcting one's own **personal information** 21
PRINCIPLE #10: COMPLIANCE 21

Consent and FIPPA **23**

Elements of a Valid Consent **23**

1. A consent must relate to the purpose for which it is being sought. 24
2. A consent must be knowledgeable – that is, it must be 'informed'. 24
3. A consent must be voluntary. 25
4. A consent must not be obtained through misrepresentation. 25
5. A consent may be subject to conditions. 25
6. A consent may be withdrawn. 25
7. A consent may be provided on behalf of an individual by an authorized person. 26

Form of Consent **27**

Privacy Provisions in FIPPA where Consent is Important **29**

Accountability and Employees, Contractors and Agents **30**

Responsibility of public bodies 30
Responsibility of a public body for its officers and staff 30
Responsibility of a public body for its contractors and agents 31

Protection of Personal Health Information - [Section 35; Subsections 1(1) and 1(2)] **33**

Collection of Personal Information - [Sections 36 and 37] 35

Overview of Sections 36 and 37 – Collection and Indirect Collection 35
Meaning of "Collect" 36
Collection – Principles and Requirements 37
Relevant Privacy Principles 37
Requirements respecting Collection of Personal Information 37

Purposes for which Personal Information May be Collected - [Subsection 36(1)] 40

Collection "by or for" a public body 40
Collection of personal information must be authorized under FIPPA 41
Collection Authorized By or Under an Enactment - [Clause 36(1)(a)] 43
1. "Enactment" 43
2. Collection authorized "by" an Act or regulation 43
3. Collection authorized "under" an Act or regulation 44
The Information Relates Directly to and is Necessary for an Existing Service, Program or Activity - [Clause 36(1)(b)] 45
A Note about Unsolicited Personal Information 47
Collection for Law Enforcement Purposes or Crime Prevention - [Clause 36(1)(c)] 48
(i) Law enforcement 48
(ii) Crime prevention 49
(iii) Collection of personal information for law enforcement purposes or crime prevention 49
A Note about Collecting Personal Information from Other Organizations 51

Limit on Amount of Personal Information Collected: Minimum Amount Necessary - [Subsection 36(2)] 52

Manner of Collection: Direct and Indirect Collection - [Subsection 37(1)] 53

Indirect Collection Authorized by the Individual or by an Enactment – [Clause 37(1)(a)] 55
(i) The individual has authorized another method of collection 55
(ii) Another enactment of Manitoba or Canada authorizes collection of personal information from a source other than the individual the information is about. 57
Direct Collection Could Harm the Individual or Others – [Clause 37 (1)(b)] 58
Reasonable expectation of harm 58
Time or Circumstance Do Not Permit Direct Collection – [Clause 37(1)(c)] 60
Direct Collection Could Result in Collection of Inaccurate Information – [Clause 37(1)(d)] 61
Personal Information May Be Disclosed to the Public Body under Division 3 – [Clause 37(1)(e)] 62
Collected for a Public Registry – [Clause 37(1)(f)] 64
Collected for Law Enforcement Purposes or Crime Prevention – [Clause 37(1)(g)] 65
(i) Law enforcement 65
(ii) Crime prevention 66
(iii) Indirect collection 67
Collected for Legal Proceedings – [Clause 37(1)(h)] 68
Collected for Use in Providing Legal Advice or Legal Services – [Clause 37(1)(i)] 70
History, Release or Supervision of an Individual in Custody, or Security of a Correctional Institution – [Clause 37(1)(j)] 72
(i) The information concerns the history, release or supervision of an individual in the custody or under the control or supervision of a correctional authority – [paragraph

37(1)(j)(i)] 72
(ii) The information concerns the security of a correctional institution - [paragraph 37(1)(j)(ii)]....74
Collected to Enforce a Family Maintenance Order – [Clause 37(1)(k)]....75
Collected to Inform the Public Guardian and Trustee or the Vulnerable Persons Commissioner – [Clause 37(1)(l)] 76
1. The Public Guardian and Trustee 76
2. The Vulnerable Persons Commissioner 77
3. Information collected to inform the Public Guardian and Trustee or the Vulnerable Persons Commissioner about a client or potential client [clause 37(1)(l)] 77
Collected to Determine or Verify Eligibility – [Clause 37(1)(m)] 78
1. Collected to determine eligibility - [Paragraph 37(1)(m)(i)] 78
2. Collected to verify eligibility - [Paragraph 37(1)(m)(ii)]....80
Determining or Collecting a Fine, Debt, Tax or Payment Owing or Making a Payment – [Clause 37(1)(n)] 81
1. Collected to determine the amount of or to collect a fine, debt, tax or payment owing to the Government of Manitoba or the public body, or an assignee of either of them - [Paragraph 37(1)(n)(i)]....81
2. Collected to make a payment - [Paragraph 37(1)(n)(ii)] 83
Collected to Manage or Administer Personnel – [Clause 37(1)(o)]....84
Collected to Audit, Monitor or Evaluate Activities – [Clause 37(1)(p)]....87
Collected to Determine Suitability for an Honour or Award – [Clause 37(1)(q)]....89
Information That Must Be Provided to the Individual: The "Privacy Notice" - [Subsections 37(2) and 37(3)]....90
1. What information must be provided to the individual 91
(i) The purpose for which the public body is collecting the information. 91
(ii) The legal authority for collecting the information. 92
(iii) The title, business address and telephone number of an officer or **employee** of the **public body** who can answer the individual's questions about the collection. 92
2. Circumstances in which the privacy notice must be given....92
3. Form of privacy notice....93

Accuracy of Personal Information - [Section 38] 95

1. "A decision that directly affects" the individual....95
2. "Reasonable steps" to ensure accuracy or completeness....96

Requests to Correct Personal Information - [section 39]....98

Overview of "Requests to Correct Personal Information" - [Section 39] 98
How to Request Correction of Personal Information - [Subsections 39(1) and 39(2)] 100
Time Limit for a Decision about Correction - [Subsections 39(3) and 39(4)] 101
Decision about Request to Correct Information - [Subsection 39(3)]....102
Duty to Notify Others - [Subsections 39(5) and 39(6)] 104

Retention of Personal Information - [Section 40]....106

1. Meaning of "Retention" 106
2. When is a public body required to establish a records retention policy under FIPPA? [Subsection 40(1)] 106
3. Content of retention policy [Subsection 40(2)]....107

4. Storage and destruction of records containing personal information 108

Protection of Personal Information - [Section 41] 110

Overview of the Duty to Protect Personal Information - [Section 41] 110
Duty to Protect Personal Information - [Section 41] 112
1. Custody or control 112
2. "Reasonable security arrangements" 113
3. " Unauthorized access" 113
4. " Unauthorized use" 115
5. "Unauthorized disclosure"" 115
6. "Unauthorized destruction" 116
7. Determining reasonable security arrangements 116
A Note on the Duty to Protect the Privacy of Access Applicants 121
What to Do If a Privacy Breach Occurs 123

Use of Personal Information - [Sections 42 and 43] 125

Overview of "Use" of Personal Information 126
Meaning of "Use" 127
Limits on Use of Personal Information - [Section 42] 129
Authorized Uses of Personal Information - [Section 43] 131
Use for the Original Purpose or for a Consistent Purpose - [Clause 43(a)] 132
1. Use for the purpose for which the personal information was originally collected or compiled 132
2. Use of personal information for a consistent purpose 133
Use with the Individual's Consent - [Clause 43(b)] 136
Use for a Purpose for which the Information May Be Disclosed to the Public Body - [Clause 43(c)] 139

Disclosure of Personal Information - [Sections 42 and 44] 140

Overview of Disclosure of Personal Information 140
Meaning of Disclosure 141
Relationship of Authorized Disclosure under Section 44 to Access to Information under Part 2 of FIPPA 142
Limits on Disclosing Personal Information - [Subsections 42(1) and (2)] 144
Authorized Disclosure of Personal Information - [Subsection 44(1)] 146
1. Disclosure of personal information must be authorized 146
2. Disclosure is authorized, or permitted, not required, under section 44 146
3. Disclosure is authorized only in the circumstances set out in subsection 44(1) 148
Disclosure for the Original or a Consistent Purpose - [Clause 44(1)(a)] 149
1. Disclosure for the purpose for which the personal information was originally collected or compiled under subsection 36(1) 149
2. Disclosure of personal information for a consistent purpose 151
Disclosure with the Individual's Consent - [Clause 44(1)(b)] 153
Disclosure in Accordance with Part 2: Access to Information - [Clause 44(1)(c)] 156
Disclosure to Comply with an Enactment or Agreement under an Enactment - [Clause 44(1)(d)] 158
1. Disclosure to comply with an enactment of Manitoba or Canada 158
2. Disclosure to comply with a treaty, arrangement or agreement entered into

under an enactment of Manitoba or Canada. 159
Disclosure Authorized or Required by an Enactment - [Clause 44(1)(e)] 161
1. Meaning of "enactment" 161
2. Disclosure authorized by an enactment 162
3. Disclosure required by an enactment 162
Disclosure to a Minister or Elected Official - [Clause 44(1)(f)] 164
Disclosure for a Common or Integrated Service, Program or Activity - [Clause 44(1)(f.1)] 166
1. Disclosure to officer or employee of a public body 167
2. "Common or integrated service, program or activity" 167
3. The information to be disclosed must be necessary to deliver the common or integrated service, program or activity. 168
4. The public body officer or employee to whom the information is disclosed must "need the information to carry out his or her responsibilities". 169
Disclosure to Manage or Administer Personnel - [Clause 44(1)(g)] 170
Disclosure to the Manitoba Auditor General, etc. for Audit Purposes - [Clause 44(1)(h)] 173
Disclosure to the Government of Canada to Monitor, Evaluate or Audit Cost Shared Programs or Services - [Clause 44(1)(i)] 175
Disclosure to Determine or Verify Suitability or Eligibility - [Clause 44(1)(j)] 176
1. Disclosure to determine suitability or eligibility for a program, service or benefit 176
2. Disclosure to verify suitability or eligibility for a program, service or benefit 177
Disclosure for Evaluation or Monitoring or for Research and Planning - [Clause 44(1)(j.1)] 178
1. Evaluating or monitoring a service, program or activity [Paragraph 44(1)(j.1)(i)] 178
2. Research and planning that relates to a service, program or activity [paragraph 44(1)(j.1)(ii)] 179
Disclosure to Enforce a Family Maintenance Order - [Section 44(1)(k)] 181
Disclosure Necessary to Protect Mental or Physical Health or Safety - [Clause 44(1)(l)] 182
Disclosure to Comply with a Subpoena, Warrant or Order - [Clause 44(1)(m)] 184
Disclosure for Legal Advice or Legal Services - [Clause 44(1)(n)] 187
Disclosure to Enforce a Legal Right - [Clause 44(1)(o)] 189
Disclosure to Determine the Amount of or Collect a Fine, Debt, Tax or Payment Owing or to Make a Payment - [Clause 44(1)(p)] 191
1. Disclosure to determine the amount of or to collect a fine, debt, tax or payment owing to the Government of Manitoba or the public body, or an assignee of either of them - [Paragraph 44(1)(p)(i)] 191
2. Making a payment [Paragraph 44(1)(p)(ii)] 194
Disclosure for Use in Legal Proceedings - [Clause 44(1)(q)] 195
Disclosure for Law Enforcement Purposes or Crime Prevention - [Clause 44(1)(r)] 197
1. Meaning of "Law enforcement" 197
2. Meaning of "Crime Prevention" 198
3. Discretion to disclose 199
Disclosure Among Law Enforcement Agencies - [Clause 44(1)(s)] 200
1. What is a law enforcement agency? 200
2. Disclosure to another law enforcement agency in Manitoba or Canada [Paragraph 44(1)(s)(i)] 201
3. Disclosure to a law enforcement agency in a foreign country - [Paragraph 44(1)(s)(ii)]. 202
Disclosure for the Purpose of Supervising an Individual in Custody - [Clause 44(1)(t)] 204

Custody 204
Control or Supervision 205
Disclosure Necessary for the Security of a Correctional Institution - [Clause 44(1)(u)] 206
Transfer to the Archives of Manitoba or to the Archives of the Public Body - [Clause 44(1)(v)] 207
Disclosure to an Officer of the Legislature - [Clause 44(1)(w)] 209
Disclosure to an Expert Under Clause 24(b) - [Clause 44(1)(x)] 211
Disclosure of Business Contact Information - [Clause 44(1)(x.1)] 212
Disclosure to a Relative in the Case of Injury, Illness or Death - [Clause 44(1)(y)] 214
Disclosure to a Relative of a Deceased Individual - [Clause 44(1)(z)] 216
Disclosure to an Information Manager - [Clause 44(1)(aa)] 218
Disclosure of Information Available to the Public - [Clause 44(1)(bb)] 219
Disclosure under Section 47 (Research Purposes) or Section 48 (Record More than 100 Years Old) - [Clause 44(1)(cc)] 220
Disclosure by an Education Institution for Fundraising - [Clause 44(1)(dd)] 222

Information Managers - [Subsection 1(1), Clause 44(1)(aa) & Section 44.1] 225

1. What is an 'information manager'? 227
2. Requirements respecting information managers 227
3. The information management agreement [Subsection 44.1(3)] 230

Disclosure for Research Purposes - [Section 47] 234

Conditions the Research Must Meet - [Clause 47(4)(b)] 236
Conditions Protecting Personal Information - [Clause 47(4)(c)] 240
Written Research Agreement Required - [Clause 47(4)(d)] 243

Disclosure of a Record Over 100 Years Old - [Section 48] 245

Privacy Impact Assessments 247

What is a "Privacy Impact Assessment"? 247
When Should a Privacy Impact Assessment be carried out? 248
Why Carry Out a Privacy Impact Assessment? 249
Some Tips on How to Approach a Privacy Impact Assessment 251
1. Gather the right team of experts, specialists and advisors. 251
2. At the outset, provide a detailed context. 251
3. Analyze, in detail, the 'information flow' using privacy principles – and the questions that flow from these principles – as the framework. 252
4. Use available tools as an aid, but don't be afraid to adjust them where necessary. 253

Chapter 6

PROTECTION OF PRIVACY

OVERVIEW

The provisions of Part 3 of FIPPA – sections 35 to 48 – deal with 'information privacy'. They protect the privacy of an individual's **personal information** by imposing obligations on **public bodies** respecting the collection, accuracy, correction, retention, destruction, protection, use and disclosure of **personal information** in their custody or under their control.

The provisions of Part 3 of FIPPA apply to **personal information** – that is, recorded information about an identifiable individual[1] – in the custody or under the control of a **public body**.[2] But, Part 3 of FIPPA does not apply:

(i) if the information is **personal health information** to which *The Personal Health Information Act* applies [section 35];

(ii) if the information is in a **record** that does not fall under FIPPA [section 4];[3] or

(iii) to the extent that another statute states that it prevails over FIPPA or that FIPPA does not apply [subsection 5(2)].[4]

A **public body** needs to take a broad and collaborative approach to protection of **personal information** in its organization, and involve individuals with a wide range of expertise – such as program managers, information technology and information security experts, records and information management experts, privacy experts and legal counsel.

Also a **public body** needs to be aware of:

(a) legislation other than FIPPA that may govern its collection, use, retention, destruction or disclosure of **personal information**. For example:

---

1 The definition **"personal information"** is discussed in Chapter 2, under *Key Definitions*.

2 The definition **"public body"** is discussed in Chapter 2, under *Public Bodies That Fall Under FIPPA*. The terms 'custody' and 'control' are discussed in Chapter 2, under *Records That Fall Under FIPPA*.

3 Section 4 is discussed in Chapter 2, under *Records That Do Not Fall Under FIPPA*.

4 Some of these statutes are discussed in Chapter 2, under *Records That Do Not Fall Under FIPPA* and under *Relationship of FIPPA to Other Legislation*.

- As noted above, some statutes state that FIPPA does not apply or that they prevail over FIPPA.
- Also, in some instances, the authority to collect, use or disclose **personal information** is expressly given in FIPPA. But as **public bodies** need to collect and maintain a wide variety of **personal information** for broad public purposes, FIPPA also recognizes that, in some cases, authority to collect, use or disclose **personal information** will be given by another statute or regulation of Manitoba or Canada. Examples are:

    - clause 36(1)(a) of FIPPA – collection authorized by or under an enactment of Manitoba or Canada[5]; and

    - clause 44(1)(e) of FIPPA – disclosure authorized or required by an enactment of Manitoba or Canada.[6]

- For government **departments** and certain **government agencies**, retention and destruction of **records** of **personal information**, is governed by *The Archives and Recordkeeping Act*.[7]

(b) other privacy legislation that may govern the organizations that the **public body** deals with. For example:

- When dealing with a private sector organization that falls under the *Personal Information Protection and Electronic Documents Act (Canada)*, the **public body** may not be able to collect **personal information** from it if the organization is not authorized to disclose the **personal information** under that federal statute.

- Federal government **departments** and agencies may not be authorized to disclose **personal information** to a **public body** unless authorized to do so under the *Privacy Act (Canada)*; etc.

---

5 Clause 36(1)(a) of FIPPA is discussed later in this Chapter, under *Collection of Personal Information*.

6 Clause 44(1)(e) of FIPPA is discussed later in this Chapter, under *Disclosure of Personal Information – Disclosure authorized or required by an enactment of Manitoba or Canada.*

7 *The Archives and Recordkeeping Act*, C.C.S.M. c. A132, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/a132e.php.

PROTECTION OF PRIVACY

This Chapter deals with:

- the "necessary, effective and proportional" test – preliminary privacy considerations when developing a new service, program, activity or initiative;
- the ten privacy principles on which Part 3 of FIPPA is based;
- consent and FIPPA;
- accountability and **employees**, contractors and agents;
- **personal health information** [section 35];
- collection of **personal information** [sections 36 and 37];
- accuracy of **personal information** [section 38];
- requests to correct **personal information** [section 39];
- retention and destruction of **personal information** [section 40];
- protection of **personal information**, including privacy breaches [section 41];
- use of **personal information** [sections 42, 43 and 45];
- disclosure of **personal information** [sections 42, 44 and 45];
- **information managers** [clause 44(1)(aa) and section 44.1];
- disclosure of **personal information** for research purposes [section 47];
- disclosure of a **record** more than 100 years old [section 48];
- privacy impact assessments.

References to the **head** of a **public body** include his or her deputy[8] and an Access and Privacy Officer to whom the **head** has delegated duties or powers under Part 3 of FIPPA.[9]

This Chapter generally follows the structure of Part 3 of FIPPA, and is meant to be read with the provisions of Part 3 of FIPPA. [10]

Note: Appendix 1 to this Manual contains a *Glossary of Terms* that includes terms defined in subsection 1(1) of FIPPA, as well as some other terms used in FIPPA or this Manual.

---

8 *The Interpretation Act* of Manitoba, clause 31(1)(d). *The Interpretation* Act, C.C.S.M. c.I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

9 The roles and responsibilities of the head of a public body, and of its Access and Privacy Officer and other officials, are discussed in Chapter 3 of this Manual.

10 In preparing this Chapter, in addition to resources cited in the footnotes, the following have been referred to:

The Government of Alberta Freedom of Information and Protection of Privacy Guidelines and Practices:
http://foip.alberta.ca/resources/guidelinespractices/index.cfm.

The Government of British Columbia Freedom of Information and Protection of Privacy Policy and Procedures Manual:
http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page.

The Government of Ontario Freedom of Information and Protection of Privacy Manual:
http://www.accessandprivacy.gov.on.ca/english/manual/index.html.

The 2005 Annotated Ontario Freedom of Information and Protection of Privacy Acts, by C. McNairn and C. Woodbury.

PRELIMINARY PRIVACY CONSIDERATIONS – NECESSARY, EFFECTIVE AND PROPORTIONAL

When a **public body** is considering a new initiative – such as a new service, program, activity or legislation – that involves collecting, using or disclosing **personal information**, a key concern is to achieve the appropriate balance between the benefits of the initiative and its impact on individual privacy.

Put another way: if an initiative involves an intrusion into privacy, a **public body** will want to consider whether the impact on privacy is 'reasonable and proportionate' in the circumstances.

The Ombudsman's three part test

The Manitoba **Ombudsman** is the independent review officer responsible for monitoring compliance with FIPPA by **public bodies**, and for promoting public awareness of FIPPA and dealing with access and privacy **complaints** under FIPPA.[11]

The **Ombudsman** has applied the following three part 'test' to determine if the balance between the benefits of an initiative and its impact on privacy has been achieved. A measure that impacts on privacy should be:

(i) necessary to achieve the intended purpose;

(ii) effective in achieving the intended purpose; and

(iii) proportional – that is:

  (a) the loss of privacy should be proportional to the benefit gained, and

  (b) there is no less privacy intrusive means of achieving the intended purpose.[12]

---

[11] The role and responsibilities of the Ombudsman under FIPPA are discussed in Chapters 7 and 8 of this Manual.

[12] See the April 30, 2000 News Release respecting the Manitoba Ombudsman's Report on the Investigation Regarding Video Surveillance in Taxicabs, found at: http://www.ombudsman.mb.ca/news/news/2003-04-30/manitoba-ombudsman-finds-that-the-collection-use-and-disclosure-of-passenger-s-images-from-taxicab-cameras-is-in-compliance-with-fippa.html.

The Privacy Commissioner of Canada has developed a very similar 4 point test:

(i) Is the measure demonstrably necessary to meet a specific need?

(ii) Is it likely to be effective in meeting that need?

(iii) Is the loss of privacy proportional to the benefit gained?

(iv) Is there a less privacy intrusive way of achieving the same end? [13]

Public bodies should consider applying these tests to new initiatives (services, programs, activities, proposed legislation, etc.) that impact on privacy as early as possible in the development process. For example, this could be done in the context of a privacy impact assessment carried out with respect to a proposed initiative.[14]

If you have any questions, contact legal counsel.

---

[13] See the Privacy Commissioner of Canada's findings in PIPEDA Case Summary #114 (January 23, 2003), found at: http://www.priv.gc.ca/cf-dc/2003/cf-dc_030123_e.cfm.

Also see PIPEDA Case Summary #290 (January 27, 2005), found at: http://www.priv.gc.ca/cf-dc/2005/290_050127_e.cfm.

And see the Fact Sheet issued by the Privacy Commissioner of Canada and the Information and Privacy Commissioner of British Columbia titled *"Privacy and Security at the Vancouver 2010 Winter Games"*, found at:. http://www.priv.gc.ca/fs-fi/02_05_d_42_ol_e.cfm.

[14] Privacy Impact Assessments are discussed later in this Chapter, under *Privacy Impact Assessments*.

THE PRIVACY PRINCIPLES IN FIPPA

Part 3 of FIPPA deals with 'information privacy' – the handling and protection of **personal information** about identifiable individuals by **public bodies**.[15]

"Personal information" means "recorded information about an identifiable individual" and includes, but is not limited to, the information listed in clauses (a) to (n) of the definition of this term in subsection 1(1) of FIPPA.[16]

The purposes of the protection of privacy provisions in FIPPA are set out in clauses 2(b), (c), (d) and (e) of FIPPA:

> (b) to allow individuals a right of access to **records** containing **personal information** about themselves in the custody or under the control of **public bodies**, subject to the limited and specific exceptions set out in this Act;
>
> (c) to allow individuals a right to request corrections to **records** containing **personal information** about themselves in the custody or under the control of **public bodies**;
>
> (d) 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**; and
>
> (e) to provide for an independent review of the decisions of **public bodies** under this Act and for the resolution of **complaints** under this Act.[17]

These purposes, and the privacy provisions of FIPPA (and of *The Personal Health Information Act*), flow from internationally recognized 'fair information principles'.

---

15 The general concept of 'Information privacy' is discussed in Chapter 1, under *Principles of Access and Privacy Legislation*.

16 The definition **"personal information"** is discussed in Chapter 2, under *Key Definitions*.

17 The purposes of FIPPA are discussed in Chapter 1, under *Purposes of FIPPA*.

In the 1980's, the international Organization for Economic Cooperation and Development issued 8 'fair information practices' (known as the OECD Privacy Guidelines).[18] These 8 principles are: collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation; and accountability. As these fair information principles are (with a bit of variation) also the basis for other public and private sector information privacy legislation in Canada, there are common 'themes' which flow through all these laws.

In November 2006, a "*Global Privacy Standard*" – a harmonization of privacy principles into a single set of fair information practices – was adopted at the International Data Protection Commissioners Conference.[19] The 10 *Global Privacy Standard* privacy principles – discussed below – are reflected in both FIPPA and *The Personal Health Information Act*.[20]

PRINCIPLE #1: CONSENT

An individual's ability to control the use and disclosure of his or her **personal information** is at the heart of 'information privacy'. Thus, free, informed and specific consent is a key privacy principle, and is reflected in both FIPPA and *The Personal Health Information Act*.

'Consent' is discussed in more detail later in this Chapter, under *"Consent and FIPPA"*.

PRINCIPLE #2: ACCOUNTABILITY

Collecting **personal information** carries with it the duty to protect the information.

Each **public body** that falls under FIPPA is responsible:

- for the **personal information** in its custody or under its control; and
- for ensuring that its **employees** – that is, its officers, staff, contractors and agents – comply with FIPPA.[21]

---

18 Canada became a signatory to the OECD Privacy Guidelines in 1984.

19 Adopted November 3, 2006. See "*Creation of a Global Privacy Standard*" by the Ontario Information and Privacy Commissioner, Ann Cavoukian, Ph.D. http://www.privacybydesign.ca/content/uploads/2010/06/gps.pdf.

20 *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

21 This responsibility is discussed later in this Chapter, under *Accountability and Employees, Contractors and Agents*.

PRINCIPLE #3: IDENTIFYING PURPOSES

A **public body** must identify the purposes for which it collects, uses, retains and discloses **personal information**.

- A **public body** can only collect **personal information** if authorized to do so by FIPPA. In order to determine if the collection is authorized under FIPPA, the purpose for which the **personal information** is being collected must first be identified.[22]

- A **public body** must limit the amount of **personal information** collected to information that is reasonably necessary to accomplish the purpose for which it is collected.[23]

- If **personal information** is collected directly from the individual it is about, the **public body** must take reasonable steps to inform the individual of the purpose for which the information is collected (as well the legal authority for the collection and who to contact with questions).[24]

- Unless use for another purpose is authorized by the individual or by FIPPA, a **public body** must only use **personal information** for the purpose for which it was collected or compiled, or for a use consistent with that purpose.[25]

- A **public body** must limit use of **personal information** to those officers, staff, contractors and agents who need to know it to carry out the authorized purpose.[26]

- Unless disclosure is authorized by the individual or by section 44 of FIPPA, a **public body** must only disclose **personal information** for the purpose for which it was collected or compiled, or for a use consistent with that purpose.[27]

- Every use and disclosure of **personal information** must be limited to the minimum amount necessary to accomplish the purpose for which it is used or disclosed.[28]

---

22 Subsection 36(1) of FIPPA, discussed later in this Chapter, under *Collection of Personal Information*.

23 Subsection 36(2) of FIPPA, discussed later in this Chapter, under *Collection of Personal Information*.

24 Clause 37(2)(a) of FIPPA, discussed later in this Chapter, under *Collection of Personal Information*.

25 Section 43 of FIPPA, discussed later in this Chapter, under *Use of Personal Information*.

26 Subsection 42(3) of FIPPA, discussed later in this Chapter, under *Use of Personal Information*.

27 Section 44 of FIPPA, discussed later in this Chapter, under *Disclosure of Personal Information*.

PRINCIPLE #4: COLLECTION LIMITATION

The term "collect" is not defined in FIPPA. To "collect" **personal information** is generally understood to mean to acquire, receive, obtain, gather, bring together or accumulate and create, by any means, a **record** of **personal information**.[29]

(a) Collection of **personal information** must be authorized.

An individual's consent does not authorize a **public body** to collect **personal information** under FIPPA.

A **public body** must find its authority to collect **personal information** in subsection 36(1) of FIPPA. That is, collection of **personal information** is only authorized under FIPPA if:

(i) collection is authorized by or under an **enactment** (a statute or regulation) of Manitoba or Canada; or

(ii) the information relates directly to and is necessary for an existing service, program or activity of the **public body**; or

(iii) the information is collected for **law enforcement** purposes or crime prevention.[30]

(b) Collection of **personal information** must be limited to the minimum amount necessary (data minimizing).

A public body can only collect "as much **personal information** as is reasonably necessary to accomplish the purpose for which it is collected".[31]

(c) **Personal information** must be collected directly from the individual it is about, unless collection of the information from another source ('indirect collection') is authorized by the individual or by FIPPA.[32]

---

28 Subsection 42(2) of FIPPA, discussed later in this Chapter, under *Use of Personal Information.* and under *Disclosure of Personal Information*.

29 The meaning of "collect" is discussed later in this Chapter, under *Collection of Personal Information*.

30 Subsection 36(1), and the authority of a public body to collect personal information, are discussed later in this Chapter, under *Collection of Personal Information*.

31 Subsection 36(2) of FIPPA, discussed later in this Chapter, under *Collection of Personal Information*.

32 Subsection 37(1) of FIPPA, discussed later in this Chapter, under *Collection of Personal Information*.

PRINCIPLE #5: USE, RETENTION AND DISCLOSURE LIMITATION

Limits on Use

The term "use" is not defined in FIPPA. "Use" is generally understood to mean dealing with **personal information** within the **public body** or for the purposes of the **public body**. In practical terms, a **public body** "uses" **personal information** when:

- its officers and staff have access to and use the **personal information** for the purposes of the **public body**. This includes situations where **personal information** is shared between the various divisions or programs of the **public body**; and

- **personal information** is collected and used by, or is shared with and used by, contractors or agents providing services to the **public body**, as the contractor or agent is receiving and using the **personal information** on behalf of the **public body**.[33]

(i) Use of **personal information** by a **public body** must be authorized.

A **public body** can only use **personal information** for the purpose for which it was collected or compiled unless:

- the individual has consented to another use; or
- use for another purpose is authorized by FIPPA.[34]

(ii) Every use of **personal information** must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used.[35]

(iii) Only those **employees** – that is, officers, staff, contractors and agents – who need to know the information to carry out the purpose for which it was collected or received, or to carry out an authorized purpose, can use **personal information**.[36]

---

33 The meaning of "use" is discussed later in this Chapter, under *Use of Personal Information*.

34 Subsection 42(1) and sections 43 and 45 of FIPPA, discussed later in this Chapter, under *Use of Personal Information*.

35 Subsection 42(2) of FIPPA, discussed later in this Chapter, under *Disclosure of Personal Information*.

36 Subsection 42(3) of FIPPA, discussed later in this Chapter, under *Use of Personal Information*.

Limits on Retention

(i) A **public body** must not retain **personal information** longer than is necessary to accomplish the purpose for which it was collected or compiled.

(ii) But, **personal information** must be retained for a reasonable period of time so that the individual it is about has a reasonable opportunity to obtain access to it.[37]

Limits on Disclosure

"Disclosure" is not defined in FIPPA. "Disclosure" is generally understood to mean revealing, showing, providing, selling or making **personal information** known to, or sharing **personal information** with, someone outside the **public body**[38]**,** by any means (for example, by providing copies, verbally, electronically or by any other means).

As each **department** of the Manitoba government is a separate **public body**, the sharing of **personal information** between government **departments** is a "disclosure" under FIPPA.

But, remember, when a **public body** shares **personal information** with a contractor or agent providing services to the **public body**, this is a "use" of the **personal information**, as the agent or contractor is acting on behalf of the **public body**.

(i) Disclosure of **personal information** by a **public body** must be authorized.[39]

A **public body** must not disclose **personal information** unless:

- the individual it is about consents, or
- the disclosure is authorized on other grounds under FIPPA.

---

37 Section 40 of FIPPA, discussed later in this Chapter, under *Retention of Personal Information*.

38 *The Concise Oxford Dictionary, 9th edition*; *Black's Law Dictionary, 6th edition*.

39 Subsection 42(1) and section 44 of FIPPA, discussed later in this Chapter, under *Disclosure of Personal Information*.

(ii) Every disclosure of **personal information** by a **public body** must be limited to the minimum amount of personal information necessary to accomplish the purpose for which it is disclosed.[40]

PRINCIPLE #6: ACCURACY

Before using **personal information** to make a decision about an individual, a **public body** must take reasonable steps to ensure that the information is accurate and complete.[41]

A **public body** must protect **personal information** in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, use, disclosure or destruction. Such arrangements include adopting reasonable physical, administrative and procedural, and technical safeguards.[42] In determining what safeguards are "reasonable", a **public body** should take into account the sensitivity of the **personal information**.

Where a person requests access under Part 2 of FIPPA – Access to Information – to a **record** containing **personal information** about someone else, the **public body** must refuse access if disclosure of the **personal information** would be an unreasonable invasion of the privacy of that other person [section 17 of FIPPA].[43]

Each **public body** that falls under FIPPA is responsible for the **personal information** in its custody or under its control, and for ensuring that its **employees** – that is, its officers, staff, contractors and agents – comply with FIPPA.[44]

PRINCIPLE #7: SECURITY – SAFEGUARDING PERSONAL INFORMATION

A **public body** must protect **personal information** in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, use, disclosure or destruction. Such arrangements include

---

40 Subsection 42(2) of FIPPA, discussed later in this Chapter, under *Disclosure of Personal Information*.

41 Section 38 of FIPPA, discussed later in this Chapter, under *Accuracy of Personal Information*.

42 Section 41 of FIPPA, discussed later in this Chapter, under *Protection of Personal Information*.

43 Section 17 of FIPPA is discussed in Chapter 5 of this Manual.

44 This responsibility is discussed later in this Chapter, under *Accountability and Employees, Contractors and Agents*.

adopting reasonable physical, administrative and procedural, and technical safeguards.[45] In determining what safeguards are "reasonable", a **public body** should take into account the sensitivity of the **personal information**.

Where a person requests access under Part 2 of FIPPA – Access to Information – to a **record** containing **personal information** about someone else, the **public body** must refuse access if disclosure of the **personal information** would be an unreasonable invasion of the privacy of that other person [section 17 of FIPPA].[46]

Each **public body** that falls under FIPPA is responsible for the **personal information** in its custody or under its control, and for ensuring that its **employees** – that is, its officers, staff, contractors and agents – comply with FIPPA.[47]

PRINCIPLE #8: OPENNESS

As information privacy is about an individual's control over his or her **personal information,** 'openness' is an important privacy principle.

Under FIPPA, when a **public body** collects **personal information** directly from the individual it is about, the **public body** must inform the individual about:

- the purpose for which the **personal information** is collected;
- the legal authority for collecting the **personal information**; and
- who to contact if the individual has questions. [48]

Public bodies should be open about their information practices and policies, and endeavour to make information about them readily available so that individuals can understand how their **personal information** is being collected, used, retained, protected, disclosed and destroyed.

---

45 Section 41 of FIPPA, discussed later in this Chapter, under *Protection of Personal Information*.

46 Section 17 of FIPPA is discussed in Chapter 5 of this Manual.

47 This responsibility is discussed later in this Chapter, under *Accountability and Employees, Contractors and Agents*.

48 Subsection 37(2) of FIPPA, discussed later in this Chapter, under *Collection of Personal Information*.

PRINCIPLE #9: ACCESS TO AND CORRECTING ONE'S OWN PERSONAL INFORMATION

Access

An individual has the right of access to his or her own **personal information** that is in the custody or under the control of a **public body**, subject only to the specific and limited exceptions set out in FIPPA.[49]

Correcting one's own **personal information**

An individual may request that a **public body** correct any **personal information** that is in its custody or under its control to which the individual has a right of access [section 39].[50]

PRINCIPLE #10: COMPLIANCE

One of the stated purposes of FIPPA is to provide for an independent review of the decisions of **public bodies**, and for the resolution of **complaints**, under FIPPA.[51] These purposes are accomplished in several ways.

(a) An individual has the right to make a **complaint** about privacy to the Manitoba **Ombudsman** if he or she believes that a **public body** has:

- collected, used or disclosed his or her **personal information** in violation of FIPPA; or
- refused to provide access to, or to correct, his or her **personal information** under FIPPA.

The **Ombudsman** is an **officer of the Legislative Assembly**, and is independent of the government. [52]

---

[49] The right of access, and the exceptions to disclosure, are discussed in Chapters 4 and 5 of this Manual.

[50] Section 39 of FIPPA, discussed later in this Chapter, under *Requests to Correct Personal Information*.

[51] Clause 2(e) of FIPPA. This provision is discussed in Chapter 1, under *Purposes of FIPPA*.

[52] The appointment and role of the Ombudsman is discussed in Chapter 7 of this Manual.

Public bodies must respond to **complaints**, cooperate with the **Ombudsman** when he or she is carrying out an investigation, and must respond to the **Ombudsman's** recommendations. The **Ombudsman's** recommendations must be made available to the public.[53]

(b) The **Ombudsman** makes recommendations, not orders. But, FIPPA has been amended to provide that, if a **public body** does not act on a recommendation of the **Ombudsman** in a privacy **complaint**, the **Ombudsman** may refer the matter to the Information and Privacy **Adjudicator**. The **Adjudicator** has the power to make an order against a **public body** that has not acted on the **Ombudsman's** recommendations. The **Adjudicator's** orders must be made available to the public.[54]

(c) Where a **complaint** is about the refusal by the **head** of a **public body** to give an individual access to his or her **personal information**, and the **Ombudsman** does not refer the **complaint** to the Information and Privacy **Adjudicator**, the individual may appeal the **public body's** refusal of access to the Manitoba Court of Queen's Bench.

(d) In addition to investigating and dealing with **complaints** under FIPPA, the **Ombudsman** is responsible for monitoring compliance with FIPPA (for example, by initiating **complaints**, conducting audits and investigations) and for promoting public awareness of protection of privacy under FIPPA.[55]

(e) FIPPA also contains offence provisions, and provides that, if a person is found guilty of an offence, the court can impose a fine of up to $50,000.

For example, it is an offence under FIPPA:

- if a person wilfully discloses **personal information** in contravention of Part 3 of FIPPA (Protection of Privacy); or
- if an **information manager** wilfully fails to comply with its obligations under FIPPA.[56]

---

53 The complaint process in FIPPA is discussed in Chapter 8 of this Manual.

54 The role of the Ombudsman and of the Information and Privacy Adjudicator in the complaint process is discussed in Chapter 8 of this Manual.

55 The role and responsibilities of the Ombudsman under FIPPA are discussed in Chapter 7 of this Manual.

56 The offence provisions in FIPPA are discussed in Chapter 3 of this Manual. The responsibilities of information managers are discussed later in this Chapter, under *Information Managers*.

CONSENT AND FIPPA

An individual's ability to control the use and disclosure of his or her **personal information** is at the heart of 'information privacy'. Thus free, informed and specific consent – the "Consent" Privacy Principle – is a key privacy principle that is reflected in FIPPA and in *The Personal Health Information Act*.[57]

Under clause 87(h) of FIPPA, the Lieutenant Governor in Council may make regulations about the giving of consents by individuals under FIPPA. At this time, there are no regulations under FIPPA about consent.

ELEMENTS OF A VALID CONSENT

As of May 1, 2010, *The Personal Health Information Act* was amended to set out the elements of a valid consent under that Act:

(i) consent must relate to the purpose for which the information is used or disclosed;

(ii) consent must be knowledgeable (that is, informed);

(iii) consent must be voluntary; and

(iv) consent must not be obtained through misrepresentation.[58]

As these elements are based on the law that has developed respecting consents generally, they are also helpful in determining what a valid consent under FIPPA is.

[57] *The Personal Health Information Act*, C.C.S.M., c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

[58] Division 2.1 of Part 3 of *The Personal Health Information Act* – Consent re Personal Health Information (sections 19.1 and 19.2).

1. A consent must relate to the purpose for which it is being sought.

A consent must clearly relate to the purpose for which it is being sought, and can only be relied on by the **public body** for that purpose.

Example:

Jack Jones consents to the disclosure of **personal information** about his financial situation by Manitoba Family Services to Manitoba Education and Advanced Learning, for the purpose of determining his eligibility for student aid. This consent cannot be relied on by Family Services as authority to disclose the **personal information** to Education and Advanced Learning for another purpose (e.g. to determine his eligibility for another Advanced Learning program, such as a training program). Nor can the consent be relied on by Advanced Learning as authority to use the information for another purpose.

2. A consent must be knowledgeable – that is, it must be 'informed'.

Consent is 'knowledgeable' or 'informed' if the individual who gives the consent has been given the information that a reasonable person in the same circumstances would need in order to decide whether to consent or not.

That is, the individual must be given enough information so that he or she understands:

- what he or she is being asked to consent to (what the consent relates to and the effect of the consent),
- the consequences that will result from giving the consent, and
- the consequences of refusing consent.

3. A consent must be voluntary.

A consent must be voluntary in the sense that the individual can choose to consent or to withhold consent.

Sometimes, the choice will seem limited. For example, there may be situations where, if a requested consent is not provided, the individual will not be eligible to receive a service or benefit. The potential for negative consequences if consent is refused does not mean that the consent is not voluntary, as the individual can still choose to give the consent, or to withhold it (and not receive the service or benefit). A consent in such circumstances is still meaningful and voluntary.[59]

4. A consent must not be obtained through misrepresentation.

5. A consent may be subject to conditions.

If a consent has been given subject to conditions, a **public body** may want to consult with legal counsel before relying on it.

6. A consent may be withdrawn.

An individual who has given a consent – in any form, express or implied – can withdraw it by notifying the **public body**.

But:

- the withdrawing of a consent does not have retroactive effect. That is, if the **public body** has acted in good faith on the basis of the consent before it is withdrawn, the withdrawal does not invalidate what the **public body** has done; and

- the individual may no longer be eligible to receive the benefit or service to which the consent related.

[59] See, for example, the Privacy Commissioner of Canada's findings in PIPEDA Case Summary #2002-65 (August 14, 2002), found at: http://www.priv.gc.ca/cf-dc/2002/cf-dc_020814_e.cfm.

7. A consent may be provided on behalf of an individual by an authorized person.

A consent may be provided on behalf of the individual the **personal information** is about in specific circumstances by a person authorized to act on the individual's behalf under section 79 of FIPPA.[60]

It is important to ensure that a person who claims he or she is authorized to consent on behalf of another is legally entitled to do so. Where there are any questions or doubts about the existence or the extent of such authority, contact legal counsel.

[60] Section 79, and the persons who are authorized to exercise rights under FIPPA on behalf of another, are discussed in Chapter 3, under *Exercising Rights on Behalf of Another Person*.

FORM OF CONSENT

A consent can be express – for example, it can be set out in a written document or conveyed by way of a clear verbal statement of consent.

A consent can also be 'implied' from the circumstances. But, a **public body** should be very cautious about relying on an 'implied consent', and it is recommended that legal counsel be consulted before doing so.

The term "authorize" is sometimes used in FIPPA instead of "consent" – for example, in clause 37(1)(a) (indirect collection may be "authorized" by the individual the information is about). In this context, the "authorization" should be express (not implied).

An express consent can be written or verbal. Where possible, a consent should be in writing. If consent is given verbally, the **public body** should make a written record of the conversation and, where reasonable, send a letter to the individual confirming the consent.

A consent under FIPPA must be clear, specific and complete. It should, amongst other things,

- clearly identify the **public body** the consent is being given to;
- fully and clearly describe the **personal information** concerned (e.g. how much of what type of **personal information** is being collected, disclosed, etc.);
- fully and clearly describe the purposes for which the consent is being sought and given (e.g. what the individual is being asked to consent to; how the information will be used; why it is necessary; the consequences of refusing the consent, etc.);
- state how long the consent will remain valid (when it expires);
- include a statement that the consent can be withdrawn by notifying the public body, and a statement explaining the consequences of withdrawing the consent;
- include the date the consent is given;
- name the person providing the consent; and
- include a signature, in the case of a written consent; etc.

As a consent provides a **public body** with legal authority to do something under FIPPA, it is strongly recommended that legal counsel be consulted when drafting a consent document.

Also, when relying on a consent as authority to do something under FIPPA, if there are any questions about the validity, meaning or scope of the consent, a **public body** should consult with legal counsel.

Also see the Ombudsman's *"Use under the Freedom of Information and Protection of Privacy Act",* [61] *regarding elements of consent for personal information under FIPPA.*

[61] The Ombudsman's Practice Note regarding elements of consent for personal information under FIPPA can be found on the Ombudsman's website at: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

■ PRIVACY PROVISIONS IN FIPPA WHERE CONSENT IS IMPORTANT

In FIPPA, an individual's consent is important in the following information privacy sections. Occasionally, the term "authorization" is used instead of "consent".

- clause 17(4)(a) and subsection 17(5) – consent to disclose **personal information** to an **applicant** for access under Part 2 – Access to Information;
- clause 37(1)(a) – authorization to collect **personal information** indirectly (that is, from someone other than the individual it is about);
- clause 43(b) – consent to use **personal information** for a purpose other than the purpose for which it was collected or compiled;
- clause 44(1)(b) – consent to disclose **personal information**;
- clause 47(4)(b)(iii) – research requests – one condition of disclosure of **personal information** for a research project is that it is unreasonable or impractical for the researcher to obtain consents to the requested disclosure;
- clause 79(a) – authorization given to another person to act on the individual's behalf.

ACCOUNTABILITY AND EMPLOYEES, CONTRACTORS AND AGENTS

Responsibility of public bodies

As noted under Privacy Principle #2 – Accountability – collecting **personal information** carries with it a duty to protect the information.

Each **public body** that falls under FIPPA is responsible for dealing with and protecting the **personal information** in its custody or under its control in accordance with the protection of privacy requirements of Part 3 of FIPPA, and for ensuring that others acting on its behalf also comply with these requirements.

In most cases, a **public body** has "custody" of a **record** of **personal information** for the purposes of FIPPA when it has physical possession of the **record**. The term "control" usually means the power or authority to make decisions about a **record**; to manage the **record**, including restricting, regulating and administering its use, disclosure or disposition.[62]

Each **public body** is responsible for ensuring that its **employees**, including its contractors and agents, comply with FIPPA.

Responsibility of a public body for its officers and staff

A **public body** is responsible for taking reasonable steps to ensure that its officers and staff comply with the protection of privacy requirements of Part 3 of FIPPA. A **public body** should:

- ensure that physical and technical measures are in place to protect **personal information**;
- ensure that administrative and procedural measures are in place to protect **personal information** – for example, by establishing policies, procedures and practices that comply with FIPPA; and
- ensure that officers and staff are aware of their responsibilities respecting **personal information** (through training, etc.),

[62] The terms 'custody' and 'control' are discussed in Chapter 2, under *Records that Fall Under FIPPA*.

Responsibility of a public body for its contractors and agents

A **public body** is also responsible for the actions of its contractors and agents.

To make this clear, the definition of **"employee"** in subsection 1(1) of FIPPA was amended to include not only the officers and staff of a **public body**, but also any person "who performs services for the **public body** under a contract or agency relationship with the **public body**" – that is, contractors and agents.[63]

A **public body** cannot avoid its responsibility under FIPPA to protect **records** and **personal information** that would ordinarily be under its control by entering into a contract with an outside organization or agent. That is, a **public body** that falls under FIPPA cannot 'contract out' of its responsibility to protect **records** and **personal information** that would ordinarily be under its control.

This means that, when entering into contracts and agreements involving **personal information** (such as contracts involving collection, use, disclosure, management, maintenance, retention or disposition of **personal information**), a **public body**:

- must not attempt to authorize the contractor or agent to do anything respecting **personal information** that the **public body** could not do under FIPPA;
- must ensure that the requirements in FIPPA respecting the **personal information** are clearly communicated to its contractor or agent in the contract or agreement; and
- must ensure that these requirements will be properly carried out, and that **personal information** will be properly protected, by its contractor or agent, through the contract or agreement and by other means.

To ensure that the **public body's** privacy obligations under FIPPA are properly dealt with in contracts and agreements, it is strongly recommended that **public bodies** consult with legal counsel – at the earliest possible stage – when drafting and negotiating such contracts and agreements.

[63] Subsection 1(1) of FIPPA. The definition of "employee" in FIPPA was amended by *The Freedom of Information and Protection of Privacy Amendment Act*, S.M. 2008 c. 40. The amending Act can be found at: http://web2.gov.mb.ca/laws/statutes/2008/c04008e.php.

If a contractor or agent is an **"information manager"** as defined in subsection 1(1) of FIPPA, it has responsibilities under FIPPA as well as responsibilities under the contract with the **public body** – but **the public body** is still responsible for the **personal information** dealt with by the **information manager** on its behalf.[64] Again, legal counsel should be involved at the earliest possible stage when drafting and negotiating an agreement with an **information manager**.

[64] The term "information manager" is defined in subsection 1(1) of FIPPA. The definition and responsibilities of information managers are similar to provisions in *The Personal Health Information Act*, and were added to FIPPA by *The Freedom of Information and Protection of Privacy Amendment Act*, S.M. 2008 c. 40. The amending Act can be found at: http://web2.gov.mb.ca/laws/statutes/2008/c04008e.php. The responsibilities of information managers are discussed later in this Chapter, under *Information Managers*.

PROTECTION OF PERSONAL HEALTH INFORMATION - [SECTION 35; SUBSECTIONS 1(1) AND 1(2)]

Part 3 of FIPPA – Protection of Privacy – does not apply to **personal health information** to which *The Personal Health Information Act* applies[65].

"Personal health information" has the same meaning in FIPPA and in *The Personal Health Information Act*. **"Personal health information"** is defined in subsection 1(1) of FIPPA as follows:[66]

> **"personal health information"** means recorded information about an identifiable individual that relates to
>
> (a) the individual's health, or health care history, including genetic information about the individual,
> (b) the provision of health care to the individual, or
> (c) payment for health care provided to the individual,
> and includes
> (d) the PHIN 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.

Subsection 1(2) of FIPPA states that, for the purposes of the definition of **personal health information** in FIPPA, "health" and "health care" have the same meaning as in subsection 1(1) of *The Personal Health Information Act*:

> "health" means the condition of being sound in mind, body and spirit;
>
> "health care" means any care, service or procedure
>
> (a) provided to diagnose, treat or maintain an individual's health,
> (b) provided to prevent disease or injury or promote health, or

---

65 Section 35 of FIPPA. For an overview of *The Personal Health Information Act*, C.C.S.M. c. P33.5, and its relationship with FIPPA, see Chapter 2, under *Relationship of FIPPA to Other Legislation*. *The Personal Health Information Act* can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

66 The definition **"personal health information"** is discussed in Chapter 2, under *Key Definitions*.

> (c) that affects the structure or a function of the body, and includes the sale or dispensing of a drug, device, equipment or other item pursuant to a prescription.

Part 3 of *The Personal Health Information Act* sets out the rules respecting collection, correction, accuracy, retention, destruction, protection, use and disclosure of **personal health information** by trustees, including **public bodies**. These rules are based on the same privacy principles that form the basis of FIPPA.

An individual seeking access to his or her own **personal health information** must request access under *The Personal Health Information Act*, not under Part 2 of FIPPA.[67]

A request by an individual to correct **personal health information** about himself or herself must be dealt with under section 12 of *The Personal Health Information Act*, not under FIPPA.

Where the **personal health information** is in a clinical record compiled and maintained in a psychiatric facility (such as the Selkirk Mental Health Centre), the rules protecting this information are in *The Mental Health Act*, not in FIPPA or *The Personal Health Information Act*.[68]

---

[67] Subsection 6(1) of FIPPA.

[68] Subsection 5(2) of FIPPA and section 39 of *The Mental Health Act*. *The Mental Health Act*, C.C.S.M. c. M110, is discussed in Chapter 2, under *Relationship of FIPPA to Other Legislation*. It can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/m110e.php.

COLLECTION OF PERSONAL INFORMATION - [SECTIONS 36 AND 37]

Reminder: **"personal information"** means "recorded information about an identifiable individual" and includes, but is not limited to, the information listed in clauses (a) to (n) of the definition of this term in subsection 1(1) of FIPPA.[69]

■ Overview of Sections 36 and 37 – Collection and Indirect Collection

Subsection 36(1) of FIPPA limits the circumstances in which, and purposes for which, **personal information**[70] may be collected by or on behalf of a **public body**.

Subsection 36(2) limits the amount of **personal information** that can be collected to the minimum amount necessary.

Subsection 37(1) directs the manner in which **personal information** is to be collected – **personal information** is to be collected directly from the individual it is about, unless the individual or FIPPA authorizes indirect collection from another source.

Subsection 37(2) requires that, where **personal information** is collected directly from the individual the information is about, the **public body** inform the individual about the purpose and legal authority for the collection, and who to contact with questions.

---

69 The definition **"personal information"** is discussed in Chapter 2, under *Key Definitions*.

70 The definition **"personal information"** is discussed in Chapter 2, under *Key Definitions*.

■ Meaning of "Collect"

To "collect" **personal information** means to assemble or accumulate **personal information**;[71] to gather **personal information** together.[72]

For the purposes of FIPPA, a **public body** "collects" **personal information** whenever it acquires, receives, obtains, gathers, brings together or accumulates and creates, by any means, a **record** of **personal information**.

Methods of collecting **personal information** include application forms and other forms, interviews, telephone calls, letters, questionnaires, public consultation processes, surveys, polls, video surveillance, etc.

Personal information may be collected by any means; collection is not restricted to any particular method, media or technology. **Personal information** may be collected in writing, by audio or video recording, by photographs, using electronic or other media, etc. For example, a **public body** that has access to **personal information** in an electronic database managed by another **public body** or organization is collecting **personal information** from that database for the purposes of FIPPA.

Collection may include the receipt of unsolicited **personal information**, such as unsolicited résumés for government positions.[73]

---

71 *The Concise Oxford Dictionary, 9th Edition*.

72 *Black's Law Dictionary, 6th Edition*.

73 Discussed later in this Chapter, under *A Note About Unsolicited Personal Information*.

■ Collection – Principles and Requirements

Relevant Privacy Principles

Four of the Privacy Principles discussed earlier in this Chapter are particularly relevant to the collection of **personal information** by **public bodies**:

- Accountability;
- Identifying Purposes;
- Collection limitation (and data minimization); and
- Openness.

Each of these principles is reflected in sections 36 and 37 of FIPPA, which deal with 'collection' of **personal information**.

Requirements respecting Collection of Personal Information

(i) A **public body** must identify the purposes for which **personal information** is to be collected.

A **public body** can only collect **personal information** for a purpose authorized under subsection 36(1) of FIPPA.

Also, the **public body** must limit the amount of **personal information** collected to the minimum amount reasonably necessary to accomplish the authorized purpose that the **public body** has identified [subsection 36(2)].

(ii) A **public body** can only collect **personal information** if it is authorized to do so under subsection 36(1) of FIPPA.

Subsection 36(1) of FIPPA limits the circumstances in which, and the purposes for which, **personal information** can be collected by a **public body**.

An individual's consent does not authorize a **public body** to collect **personal information** under FIPPA.

A **public body** must find its authority to collect **personal information** in subsection 36(1) of FIPPA. That is, collection of **personal information** is only authorized under FIPPA if:

(a) collection is authorized by or under an **enactment** (statute or regulation) of Manitoba or Canada; or

(b) the information relates directly to and is necessary for an existing service, program or activity of the **public body**; or

(c) the information is collected for **law enforcement** purposes or crime prevention.[74]

(iii) A **public body** can only collect "as much **personal information** as is reasonably necessary to accomplish the purpose for which it is collected" [subsection 36(2)].

That is, the **public body** must limit the amount of **personal information** collected to the minimum amount reasonably necessary to accomplish the authorized purpose that the **public body** has identified.

(iv) A **public body** must collect **personal information** directly from the individual it is about, unless the individual or FIPPA authorizes the **public body** to collect the information from another source ('indirect collection') [subsection 37(1)].

(v) When a **public body** collects **personal information** directly from the individual it is about, the **public body** must inform the individual of:

(a) the purpose for which the **personal information** is collected;
(b) the legal authority for collecting the **personal information**; and
(c) who to contact if the individual has questions [subsection 37(2)].

(vi) **Personal information** can be collected "by" a **public body** or "for" (on behalf of) the **public body** by another (e.g. a contractor, agent, etc.) [subsection 36(1)].

[74] Subsection 36(1), and the authority of a public body to collect personal information, are discussed later in this Chapter, under *Collection of Personal Information*.

(vii) Collecting **personal information** carries with it the duty to protect the information [section 41].

A **public body** is responsible not only for the collection of **personal information** by its officers and staff, but also for the actions of its contractors and agents when they collect **personal information** "for" (on behalf of) the **public body**. When dealing with contractors or agents, a **public body** must ensure that the **personal information** is properly protected, through contractual and other means.[75]

FIPPA now provides that, if a contractor or agent is an "**information manager**" as defined in subsection 1(1), the contractor or agent will have responsibilities under FIPPA as well as under its contract with the **public body** – but the **public body** is still responsible for any **personal information** collected by the **information manager** on its behalf.[76]

Public bodies should regularly review their activities to ensure that **personal information** is being collected in accordance with FIPPA.

Also see Manitoba Ombudsman Practice Note: *Collection and Providing Notice of Collection of Personal Information under FIPPA*.[77]

[75] This responsibility is discussed earlier in this Chapter, under *Accountability and Employees, Contractors and Agents*.

[76] The definition and responsibilities of 'information managers' are discussed later in this Chapter, under *Information Managers*.

[77] This Practice Note can be found on the Ombudsman's website: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html. .

■ PURPOSES FOR WHICH PERSONAL INFORMATION MAY BE COLLECTED - [SUBSECTION 36(1)][78]

Subsection 36(1) of FIPPA limits the circumstances in which, and purposes for which, **personal information**[79] may be collected by or on behalf of a **public body**.

Subsection 36(2) limits the amount of **personal information** that can be collected to the minimum amount necessary.

> **Purpose of collection of information**
> **36(1)** No **personal information** may be collected by or for a **public body** unless
>
> (a) collection of the information is authorized by or under an **enactment** of Manitoba or of Canada;
>
> (b) the information relates directly to and is necessary for an existing service, program or activity of the **public body**; or
>
> (c) the information is collected for **law enforcement** purposes or crime prevention.

Collection "by or for" a public body

Under subsection 36(1), collection of **personal information** can be carried out:

- by the **public body** itself (through its officers or staff), or

---

[78] Subsection 13(1) of *The Personal Health Information Act* limits the collection of **personal health information** by trustees, including **public bodies**. Section 26 of that Act restricts the collection of the Personal Health Identification Number (PHIN), and applies to all persons, not just trustees or **public bodies**. *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

[79] The definition **"personal information"** is discussed in Chapter 2, under *Key Definitions*.

- "for" the **public body**; that is, on behalf of the **public body** by another such as a contractor or agent under a contract, agreement or arrangement. For example, one Manitoba government **department** can collect **personal information** "for" (on behalf of) another **department** under an agency arrangement.

A **public body** must comply with the requirements of FIPPA whether it collects the **personal information** itself or authorizes a contractor or agent to carry out the collection on its behalf.[80]

A **public body** is responsible for the actions of its contractors and agents and must ensure that the **public body's** obligations respecting collection of **personal information** are being met by its contractor or agent, and that the **personal information** is properly protected, through contractual and other means.

With changes to FIPPA on January 1, 2011, FIPPA provides that, if a contractor or agent is an **"information manager"** as defined in subsection 1(1), the contractor or agent will have responsibilities under the FIPPA as well as under its contract with the **public body** – but the **public body** is still responsible for any **personal information** collected by the **information manager** on its behalf.[81]

It is strongly recommended that **public bodies** involve legal counsel when developing or negotiating a contract, agreement or arrangement involving collection of **personal information** on its behalf.

Collection of personal information must be authorized under FIPPA

Personal information cannot be collected "by or for" a **public body** unless the collection is authorized under one of clauses 36(1)(a), (b) or (c) of FIPPA.

In order to determine if collection is authorized under clause 36(1)(a),(b) or (c), the **public body** must first identify the purposes for which the **personal information** is to be collected.

---

80 This responsibility is discussed earlier in this Chapter, under *Accountability and Employees, Contractors and Agents*.

81 The definition and responsibilities of "information managers" are discussed later in this Chapter, under *Information Managers*.

Note: an individual's consent does not authorize a **public body** to collect **personal information** under FIPPA. A **public body** must find its authority to collect **personal information** in one of clauses 36(1)(a), (b) or (c) of FIPPA.

■ Collection Authorized By or Under an Enactment - [Clause 36(1)(a)]

> **Purpose of collection of information**
> **36(1)** No **personal information** may be collected by or for a **public body** unless
>
> (a) collection of the information is authorized by or under an **enactment** of Manitoba or of Canada;

Clause 36(1)(a) states that **personal information** may be collected by or on behalf of a **public body** if collection of the information is authorized:

- by an **enactment** of Manitoba or Canada; or
- under an **enactment** of Manitoba or Canada.

1. "Enactment"

"Enactment" is defined in subsection 1(1) of FIPPA as "an Act or regulation".

For the purposes of clause 36(1)(a):

- an "Act" is a statute passed by the Legislative Assembly of Manitoba or by the Parliament of Canada; and
- a "regulation" is a law made under the authority of a statute by the Lieutenant Governor in Council (in the case of Manitoba), the Governor General in Council (in the case of Canada), a minister, etc.

2. Collection authorized "by" an Act or regulation

Collection of **personal information** is authorized "by" an Act or a regulation where the Act or regulation describes the type of **personal information** that can be collected by, or that is to be provided to, the **public body** (e.g. name, address, birth date, etc.).

In these situations, the Act or regulation authorizes collection of **personal information** and also limits the **personal information** that can be collected to the type of information described.

Example:

Subsection 2(2) of *The Change of Name Act* specifies the information that must be provided to the Director of the Vital Statistics Agency as part of an application for a change of name.

3. Collection authorized "under" an Act or regulation

Often, an Act or regulation simply gives authority to establish or carry out a program, service or activity for which **personal information** is needed, but does not describe the type of information that may be collected.

In these circumstances, the collection of **personal information** is impliedly authorized "under" the Act or regulation, but the **public body** will have to determine exactly what **personal information** is required to carry out the program, service or activity. In doing so, the **public body** must keep in mind the requirement in subsection 36(2) of FIPPA to collect only as much **personal information** about an individual as is reasonably necessary to accomplish the purpose for which it is collected.[82]

Example:

The regulation under *The Legal Aid Manitoba Act* requires that an application for legal aid benefits be in writing in a form approved by Legal Aid Manitoba.

[82] Subsection 36(2) is discussed later in this Chapter, under *Limit on Collection: Minimum Amount Necessary*.

■ The Information Relates Directly to and is Necessary for an Existing Service, Program or Activity - [Clause 36(1)(b)]

> **Purpose of collection of information**
> **36(1)** No **personal information** may be collected by or for a **public body** unless
>
> (b) the information relates directly to and is necessary for an existing service, program or activity of the **public body**;

Clause 36(1)(b) permits the collection of **personal information** if that information relates directly to and is necessary for an existing service, program or activity of the **public body** that is collecting the **personal information**, or on whose behalf the **personal information** is collected.

There are three requirements in clause 36(1)(b), all of which must be met for collection of **personal information** to be authorized under this clause:

*(i) The **personal information** collected must "relate directly to" a service, program or activity.*

Personal information relates directly to a service, program or activity if it has a direct or unambiguous[83] bearing on or connection or relevance[84] to the service, program or activity.

*(ii) The **personal information** collected must be "necessary for" the service, program or activity.*

Personal information is necessary for a service, program or activity if it is required for or essential to the service, program or activity.[85]

---

83 *The Concise Oxford Dictionary, 9th Edition*.

84 *Black's Law Dictionary, 6th Edition*.

85 *The Concise Oxford Dictionary, 9th Edition*.

A **public body** must determine the exact elements of **personal information** that it needs to properly deliver or carry out a service, program or activity, and must limit collection to only as much **personal information** as is necessary to do so. That is, the **public body** should be able to establish that:

- there is a reasonable basis for collecting the **personal information**; and

- it has a 'need to know' each element of **personal information** being collected to properly deliver or carry out that particular service, program or activity. FIPPA does not permit collection of **personal information** "just in case" it might be needed for the service, program or activity in the future.

*(iii) The **personal information** must be collected for an "existing" service, program or activity of the **public body** that is collecting the **personal information**, or on whose behalf it is collected.*

The service, program or activity must be in place at the time the **personal information** is collected. FIPPA does not permit collection of **personal information** in anticipation of a program or activity that may come into effect or that may be carried out some time in the future. That is, FIPPA does not permit collection of **personal information** "just in case" it might be needed for some activity in the future.

The service, program or activity must be a service, program or activity of the **public body** collecting the **personal information**, or on whose behalf it is collected.

But, the service, program or activity does not have to be established under the authority of a specific statute or regulation for clause 36(1)(b) to apply. An example of a program that may not be established under the authority of a specific statute or regulation is an employment equity program of a **public body**.

A Note about Unsolicited Personal Information

If a **public body** receives unsolicited **personal information** that does not relate to, and is not necessary for, an existing service, program or activity, the **public body** may want to consider whether adopting a policy of returning the **personal information** (in a secure manner) would be appropriate.

There may be some situations where a **public body** might want to keep unsolicited **personal information** for a specified period of time before destroying it in accordance with a records schedule approved under *The Archives and Recordkeeping Act*[86] – for example, unsolicited résumés.

[86] *The Archives and Recordkeeping Act*, C.C.S.M. C. A132, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/a132e.php.

■ Collection for Law Enforcement Purposes or Crime Prevention - [Clause 36(1)(c)]

> **Purpose of collection**
> **36(1)** No **personal information** may be collected by or for a **public body** unless
>
> (c) the information is collected for **law enforcement** purposes or crime prevention.

Clause 36(1)(c) permits collection of **personal information** by or on behalf of a **public body** for either of two purposes:

(i) for **law enforcement** purposes; or

(ii) for crime prevention.

(i) Law enforcement

"Law enforcement" is defined in subsection 1(1) of FIPPA:

> **"law enforcement"** means any action taken for the purpose of enforcing an **enactment**, including
>
> (a) policing,
>
> (b) investigations or inspections that lead or could lead to a penalty or sanction being imposed, or that are otherwise conducted for the purpose of enforcing an **enactment**, and
>
> (c) proceedings that lead or could lead to a penalty or sanction being imposed, or that are otherwise conducted for the purpose of enforcing an **enactment**;[87]

[87] The definition **"law enforcement"** is discussed in Chapter 2, under *Key Definitions*.

"Law enforcement" is not limited to the investigative activities of police forces, but also includes a wide variety of investigations and actions by **public bodies**, if they are undertaken for the purpose of enforcing an **enactment**.

"Enactment" is defined in subsection 1(1) of FIPPA as "an Act or regulation".

- An "Act" is a statute passed by the Legislative Assembly of a province or by the Parliament of Canada.
- A regulation is a law made under the authority of a statute by the Lieutenant Governor in Council (in the case of a province), the Governor General in Council (in the case of Canada), a minister, etc.

Examples of **law enforcement** include:

- safety inspections under *The Workplace Safety Act;*
- investigations by the Office of the Fire Commissioner;
- the regulatory activities of the Superintendent of Insurance;
- investigations under *The Human Rights Code* of Manitoba;
- investigations by child and family services agencies to determine if a child is in need of protection under *The Child and Family Services Act*; etc.

(ii) Crime prevention

"Crime prevention" is prevention of conduct that society's laws prohibit.[88]

(iii) Collection of personal information for law enforcement purposes or crime prevention

[88] Definition of "crime" from *The Dictionary of Canadian Law*.

Clause 36(1)(c) of FIPPA recognizes that **law enforcement** agencies must engage in wide ranging information collection that may not always fall comfortably under clause 36(1)(b). For example, it could be difficult for a **law enforcement** agency to show, at the moment of collection, how each piece of **personal information** collected for investigative or enforcement purposes relates directly to or is necessary for the activity under way – this may only become apparent after a great deal of information is assembled. Also, certain investigative methods, such as taking witness statements, could be seriously compromised.

Note:

If a **public body** is authorized to collect **personal information** for **law enforcement** purposes or for crime prevention under clause 36(1)(c) of FIPPA, the **public body** is also authorized to collect the **personal information** indirectly – that is, from sources other than the individual the information is about – under clause 37(1)(g) of FIPPA.

A Note about Collecting Personal Information from Other Organizations

A **public body** must be aware of other privacy statutes and regulations that may govern the organizations that the **public body** deals with.

For example, a **public body** may not be able to collect **personal information**:

- from another **public body** that falls under FIPPA, if that other **public body** does not have authority to disclose the **personal information** to it under subsection 44(1) of FIPPA;

- from a federal government institution that falls under the *Privacy Act (Canada)*, if that institution is not authorized to disclose the **personal information** to the **public body** under the *Privacy Act (Canada)*;

- a private sector organization that falls under the *Personal Information Protection and Electronic Documents Act (Canada)*, if that organization is not authorized to disclose the **personal information** to the **public body** by that federal Act.

LIMIT ON AMOUNT OF PERSONAL INFORMATION COLLECTED: MINIMUM AMOUNT NECESSARY - [SUBSECTION 36(2)][89]

> **Limit on amount of information collected**
> **36(2)** A **public body** shall collect only as much **personal information** about an individual as is reasonably necessary to accomplish the purpose for which it is collected.

Subsection 36(2) contains a very important limit on collection: a **public body** must collect only as much **personal information** as is reasonably necessary to accomplish the purpose for which it is permitted to be collected under clause 36(1)(a), (b) or (c) of FIPPA. That is, when collecting **personal information**, and when **personal information** is collected on its behalf, a **public body** must only collect the 'minimum amount' of **personal information** necessary to accomplish the identified, authorized purpose for which the information is being collected.

If a **public body** collects more **personal information** than is necessary to accomplish the authorized purpose – commonly referred to as 'over collection' – the **public body** is not complying with FIPPA.

A **public body** should regularly review its collection practices, and have measures in place, to ensure that it is collecting the minimum amount of **personal information** necessary for the identified, authorized purpose. This can include:

- reviewing and redesigning forms, questionnaires and procedures used to gather **personal information**;
- developing and reviewing policy manuals and procedures manuals;
- reviewing contracts, agreements and arrangements with contractors and agents who collect **personal information** on behalf of the **public body**, etc.

[89] Subsection 13(2) of *The Personal Health Information Act* also limits the amount of **personal health information** that may be collected by a trustee, including a **public body**, to the minimum amount necessary to accomplish the authorized purpose for which it is collected.

■ MANNER OF COLLECTION: DIRECT AND INDIRECT COLLECTION - [SUBSECTION 37(1)][90]

The terms 'direct collection' and 'indirect collection' are not defined in FIPPA. 'Direct collection' refers to collecting **personal information** directly from the individual the information is about. 'Indirect collection' refers to collecting **personal information** from a source other than the individual the information is about.

> **Manner of collection**
> **37(1)** **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless

Subsection 37(1) governs who a **public body** may collect **personal information** from. **Personal information** must be collected directly from the individual it is about, unless collection of the **personal information** from another source (indirect collection) is:

- authorized by the individual the information is about [clause 37(1)(a)]; or
- authorized under one of the other circumstances described in clauses 37(1)(a) to (q) of FIPPA.

This requirement to collect **personal information** directly from the individual it is about applies whether the **personal information** is collected by the **public body** itself, or is collected for (on behalf of) the **public body** by someone else, such as a contractor or agent, to collect the information on its behalf.

---

[90] Subsection 14(1) of *The Personal Health Information Act* provides that a trustee, including a **public body**, must collect **personal health information** directly from the individual the information is about wherever possible, unless collection from another source is authorized under clause 14(2)(a), (b), (c), (c.1), (d), (d.1) or (e) of that Act. *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

The 'direct collection' requirement is an important aspect of the "Openness" Privacy Principle (Principle #8), as it is intended to ensure that an individual is generally aware of the **personal information** that a **public body** is collecting about him or her. To exercise the privacy rights under Part 3 of FIPPA, such as the right to request a correction of **personal information** or to complain if the information is being used or disclosed in a manner not authorized by FIPPA, an individual must have some idea as to the nature of the **personal information** being collected about him or her.

Personal information can be collected by or for a **public body** from sources other than the individual the information is about – that is, 'indirectly' – only in the circumstances described in clauses 37(1)(a) to (q) of FIPPA.

Example:

When **Public Body** X collects **personal information** from a person or body other than the individual the information is about, **Public Body**X:

(a) needs authority to collect the **personal information** under subsection 36(1); and

(b) also needs authority to collect the **personal information** indirectly under subsection 37(1) of FIPPA – that is, it needs authority to collect the information from a source other than the individual the information is about.

If **Public Body** X is collecting the **personal information** from **Public Body** Y (another **public body** that also falls under FIPPA):

(c) **Public body** Y also needs authority to disclose the **personal information** to **Public Body** X under subsection 44(1) of FIPPA.

■ Indirect Collection Authorized by the Individual or by an Enactment – [Clause 37(1)(a)]

Manner of collection
37(1) **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless

(a) another method of collection is authorized by that individual, or by an **enactment** of Manitoba or Canada;

Under clause 37(1)(a), a **public body** may collect **personal information** from sources other than the individual the information is about in either of two situations:

(i) if the individual the **personal information** is about has authorized another method of collecting his or her **personal information**; or

(ii) if an **enactment** of Manitoba or Canada authorizes another method of collecting the **personal information**.

(i) The individual has authorized another method of collection

The individual the **personal information** is about may "authorize" a **public body** to collect his or her **personal information** from someone else. For example, an individual might authorize Manitoba Student Aid to collect financial information about him or her from the Canada Revenue Agency.

The term "authorize" is not defined in FIPPA, but in this context it is generally understood to mean that the individual is "expressly consenting" to the **public body** collecting his or her **personal information** from other sources.

To be valid, the authorization must meet the requirements of a valid consent.[91] That is, the authorization:

(i) must relate to the indirect collection for which authorization is being sought;

(ii) must be knowledgeable (that is, informed);

(iii) must be voluntary; and

(iv) must not be obtained through misrepresentation.

Where reasonable, an individual's authorization to collect **personal information** from other sources should be in writing. If authorization is given verbally, the **public body** should make a written record of the conversation and, where reasonable, send a letter to the individual confirming the authorization.

The individual's authorization (verbal or written) should ordinarily include:

- a description of the **personal information** to be collected by the **public body** (e.g. how much of what type of **personal information** is being collected);
- the source or sources from which that **personal information** is to be collected;
- the identity of the **public body** collecting the **personal information**;
- the purpose of the collection of the **personal information** (e.g. why the **personal information** is necessary, what the **personal information** will be used for, etc.);
- if appropriate, the reasons for collecting the **personal information** indirectly;
- the date the authorization expires; and
- the consequences of refusing to authorize the indirect collection.

[91] Consents under FIPPA are discussed earlier in this Chapter, under *Consent and FIPPA*.

Authorization to collect **personal information** from other sources, in specific circumstances, may be given by a person authorized to act on behalf of another under section 79 of FIPPA.[92]

Also see the Ombudsman's *" Use under the Freedom of Information and Protection of Privacy Act",* [93] *regarding elements of consent for personal information.*

(ii) Another enactment of Manitoba or Canada authorizes collection of personal information from a source other than the individual the information is about.

A **public body** may collect **personal information** from a source other than the individual the information is about if authorized to do so by another **enactment** of Manitoba or an **enactment** of Canada.

"Enactment" is defined in subsection 1(1) of FIPPA as "an Act or regulation". For the purposes of clause 37(1)(a):

- an "Act" is a statute passed by the Legislative Assembly of Manitoba or by the Parliament of Canada; and
- a "regulation" is a law made under the authority of a statute by the Lieutenant Governor in Council (in the case of Manitoba), the Governor General in Council (in the case of Canada), a minister, etc.

92 Section 79 is discussed in Chapter 3, under *Exercising Rights on Behalf of Another*.

93 The Ombudsman's Practice Note regarding elements of consent for personal information under FIPPA can be found on the Ombudsman's website at: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

■ Direct Collection Could Harm the Individual or Others – [Clause 37 (1)(b)]

> **Manner of collection**
> **37(1)** **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless
>
> (b) collection of the information directly from the individual could reasonably be expected to cause harm to the individual or to another person;

Clause 37(1)(b) authorizes a **public body** to collect **personal information** from a source other than the individual the information is about if collection directly from the individual could reasonably be expected to:

(i) cause harm to that individual; or

(ii) cause harm to another person.

"Harm" means hurt or damage.[94]

"Person" means a natural person (a human being) and also includes a corporation and the heirs, executors, administrators or other legal representatives of a person.[95]

Reasonable expectation of harm

Whether or not collection of **personal information** directly from the individual it is about "could reasonably be expected" to harm that individual or another person is a question of fact that must be determined after taking into account all the relevant circumstances.

---

94 *The Concise Oxford Dictionary, 9th Edition*.

95 *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act*, C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

The expectation of harm must be reasonable. Reasonableness is judged by an objective standard. A 'reasonable expectation' is one that is not fanciful, imaginary or contrived, but rather one that is based on reason.[96]

In short, the 'reasonable expectation of harm' test requires that the facts and circumstances establish a likelihood that harm will result to the individual or another person if the **personal information** is collected directly from the individual it is about.

Example:

If collecting sensitive **personal information** directly from a person applying for a benefit such as social assistance is clearly causing him or her serious distress, it may be advisable to try to collect the necessary information from a family member.

[96] Ontario Information and Privacy Commissioner, Order P-203 (Re Stadium Corp. of Ontario, Nov. 5, 1990) (made in the context of an application for access to information). http://ipc.on.ca/images/Findings/Attached_PDF/P-203.pdf.

■ Time or Circumstance Do Not Permit Direct Collection – [Clause 37(1)(c)]

Manner of collection

37(1) **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless

(c) collection of the information is in the interest of the individual and time or circumstances do not permit collection directly from the individual;

Clause 37(1) contains two requirements, both of which must be met for the clause to apply:

(i) collection of the **personal information** must be in the interest of the individual the information is about.

In other words, there must be some benefit to the individual that will result from the collection of the **personal information**; and

(ii) time or circumstances do not permit collection of the **personal information** directly from the individual the information is about.

For example, there is some element of urgency.

Example:

Under this clause a hospital (a **local public body**) could obtain the name and address of the next of kin of an unconscious individual involved in a workplace accident from the individual's employer for the purpose of notifying family members of the accident.

■ Direct Collection Could Result in Collection of Inaccurate Information – [Clause 37(1)(d)]

> **Manner of collection**
> **37(1)** **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless
>
> (d) collection of the information directly from the individual could reasonably be expected to result in inaccurate information being collected;

"Inaccurate" information means information that is not correct or not complete.

Whether or not collection of **personal information** directly from the individual it is about "could reasonably be expected" to result in inaccurate information being collected is a question of fact that must be determined after taking into account all the relevant circumstances. The expectation must be reasonable. Reasonableness is judged by an objective standard. A 'reasonable expectation' is one that is not fanciful, imaginary or contrived, but rather one that is based on reason. [97]

In short, the facts and information must establish a probability or likelihood that collection of the **personal information** from the individual it is about will result in incorrect or incomplete information. Clause 37(1)(d) should be used in limited circumstances.

[97] Ontario Information and Privacy Commissioner, Order 203 (Re Stadium Corp. of Ontario, Nov. 5, 1990), made in the context of an application for access to information: http://ipc.on.ca/images/Findings/Attached_PDF/P-203.pdf.

■ Personal Information May Be Disclosed to the Public Body under Division 3 – [Clause 37(1)(e)]

> **37(1)** **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless
>
> (e) the information may be disclosed to the **public body** under Division 3 of this Part;

Clause 37(1)(e) allows a **public body** to indirectly collect **personal information** that another **public body** is authorized to disclose to it under Division 3 of FIPPA.

Sections 44 to 48 of Division 3 of FIPPA set out the situations when a **public body** is permitted to disclose **personal information** under FIPPA.[98]

"Disclose" is not defined in FIPPA. To "disclose" **personal information** is generally understood to mean revealing, showing, providing, selling or making **personal information** known to, or sharing **personal information** with, someone outside the **public body**[99] by any means (for example, by providing copies, verbally, electronically or by any other means).

Any sharing of **personal information** with another government **department** or another **public body** is a disclosure of **personal information** that must be authorized under section 44, 44.1, 47 or 48 of FIPPA.[100]

---

98 Disclosure of personal information, and sections 44 to 48, are dealt with later in this Chapter, under *Disclosure of Personal Information*.

99 *The Concise Oxford Dictionary, 9th edition*; *Black's Law Dictionary, 6th edition*.

100 Disclosure of personal information, and sections 44 to 48 of FIPPA, are discussed later in this Chapter under *Disclosure of Personal Information*.

Clause 37(1)(e) recognizes that there are limited circumstances where it is appropriate for **public bodies** to share **personal information**, particularly where the same **personal information** is required by more than one **public body** for legitimate services, programs and activities. In appropriate circumstances, this clause can reduce the number of times an individual must provide the same **personal information** to more than one **public body** and can reduce the cost of gathering **personal information** required by more than one **public body**.

As each **department** of the Manitoba government is a separate **public body**, the sharing of **personal information** between government **departments** is a "disclosure" under FIPPA.

Example:

Clause 37(1)(e) permits Department A to indirectly collect **personal information** from Department B, if Department B is authorized to disclose the information to Department A.

Remember: Department A must also be authorized to collect the **personal information** under subsection 36(1) of FIPPA.

Remember:

When a **public body** shares **personal information** with a contractor or agent providing services to the **public body**, this is a "use" of the **personal information**, not a disclosure, as the agent or contractor is acting on behalf of the **public body**.[101]

[101] Use of personal information is discussed later in this Chapter, under *Use of Personal Information*.

■ Collected for a Public Registry – [Clause 37(1)(f)]

Manner of collection

37(1) **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless

(f) the information is collected for inclusion in a public registry;

With changes to FIPPA on January 1, 2011, the term "public registry" is no longer defined. But it would generally be understood to mean a registry of information that is maintained by a **public body** and that is available to the public, or a segment of the public.

Examples of public registries include: *The Real Property Act* Registry; the Personal Property Registry; the Corporations Registry; the Change of Name Registry; the Driving Schools Registry; the Liquor Control Commission's Licensed Premises Registry; etc.

There are many situations where **personal information** to be filed or registered in a **public registry** will come from a source other than the individual the information is about.

Example:

A creditor may register a financing statement showing the debt owing to the creditor by another individual (the debtor) in the Personal Property Registry established under *The Personal Property Security Act*.

■ Collected for Law Enforcement Purposes or Crime Prevention – [Clause 37(1)(g)]

> **Manner of collection**
> **37(1)** **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless
>
> (g) the information is collected for **law enforcement** purposes or crime prevention;

Clause 37(1)(g) permits a **public body** to collect **personal information** from a source other than the individual the information is about for either of two purposes:

(i) **law enforcement** purposes; or

(ii) crime prevention.

(i) Law enforcement[102]

"**Law enforcement**" is defined in subsection 1(1) of FIPPA:

> **"law enforcement"** means any action taken for the purpose of enforcing an **enactment**, including
>
> (a) policing,
>
> (b) investigations or inspections that lead or could lead to a penalty or sanction being imposed, or that are otherwise conducted for the purpose of enforcing an **enactment**, and

[102] The meaning of "law enforcement" is discussed in Chapter 2, under *Key Definitions*.

> (c) proceedings that lead or could lead to a penalty or sanction being imposed, or that are otherwise conducted for the purpose of enforcing an **enactment**.

"Law enforcement" is not limited to the investigative activities of police forces, but also includes a wide variety of investigations and actions by **public bodies**, if they are undertaken for the purpose of enforcing an **enactment**.

"Enactment" is defined in section 1 of FIPPA as "an Act or regulation".

- An "Act" is a statute passed by the Legislative Assembly of a province or by the Parliament of Canada.
- A "regulation" is a law made under the authority of a statute by the Lieutenant Governor in Council (in the case of a province), the Governor General in Council (in the case of Canada), a minister, etc.

Examples of **law enforcement** include:

- safety inspections under *The Workplace Safety Act*;
- investigations by the Office of the Fire Commissioner;
- the regulatory activities of the Superintendent of Insurance;
- investigations under *The Human Rights Code* of Manitoba;
- investigations by child and family services agencies to determine if a child is in need of protection under *The Child and Family Services Act*; etc.

(ii) Crime prevention

"Crime prevention" is prevention of conduct that society's laws prohibit.[103]

[103] Definition of "crime" from *The Dictionary of Canadian Law*.

(iii) Indirect collection

If a **public body** is authorized to collect **personal information** for **law enforcement** purposes or for crime prevention under clause 36(1)(c) of FIPPA, the **public body** is also authorized to collect the **personal information** indirectly – that is, from sources other than the individual the information is about – under clause 37(1)(g) of FIPPA.

Clause 37(1)(g) allows a **public body** involved in **law enforcement** or crime prevention to collect **personal information** from sources other than the individual the information is about.

Often, an investigator may not want to alert an individual to the fact that an investigation is taking place, as the individual might alter, remove or destroy evidence. Also, information relevant to **law enforcement** or crime prevention may have to be collected from other sources to ensure accuracy.

■ Collected for Legal Proceedings – [Clause 37(1)(h)]

Manner of collection
37(1) **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless

(h) the information is collected for the purpose of existing or anticipated legal proceedings to which the Government of Manitoba or the **public body** is a party;

Clause 37(1)(h) allows a **public body** to collect **personal information** from a source other than the individual the information is about if the information is collected for the purpose of:

(i) existing legal proceedings to which the Government of Manitoba or the **public body** collecting the **personal information** is a party; or

(ii) anticipated legal proceedings to which the Government of Manitoba or the **public body** collecting the **personal information** is a party.

Clause 37(1)(h) recognizes that legal counsel and those assisting counsel may, in preparing for or conducting legal proceedings, need to collect **personal information** from sources other than the person the information is about. In some circumstances, attempts by legal counsel to collect information directly from the individual the information is about may result in information being withheld or destroyed or in inaccurate information being provided, or the individual may not have the information necessary.

A "legal proceeding" is any civil or criminal proceeding or inquiry in which evidence is or may be given, and includes an arbitration;[104] any proceeding authorized or sanctioned by law, and brought or instituted, for the acquiring of a right or the enforcement of a remedy.[105]
Clause 37(1)(h) applies where:

[104] *The Dictionary of Canadian Law.*

[105] *Black's Law Dictionary, 6th Edition.*

- the **public body** collecting the **personal information** is a party to the existing or anticipated legal proceedings; or

- the Government of Manitoba, in the broad, 'corporate' sense, is a party to the proceedings.

The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[106] and is a broader concept than **"department"** or **public body**. Usually, legal proceedings involving a government **department** or **departments** are brought against "The Government of Manitoba" and not against individual **departments**.[107]

The **personal information** may be collected:

- by the **public body** concerned;

- by legal counsel acting for (on behalf of) the **public body** or the Government (including Crown Counsel or Crown Prosecutors in Manitoba Justice; staff legal counsel; private bar legal counsel retained by the **public body** or the Government; etc.); or

- by persons assisting legal counsel in preparing for or conducting the legal proceedings on behalf of the **public body** or the Government (including experts, investigators, etc.).

There is some overlap between clause 37(1)(h) and clause 37(1)(i) – indirect collection for use in providing legal advice or services.

---

106 *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act*, C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

107 *The Proceedings Against the Crown Act*, C.C.S.M. c. P140, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p140e.php.

■ Collected for Use in Providing Legal Advice or Legal Services – [Clause 37(1)(i)]

> **37(1)** **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless
>
> (i) the information is collected for use in providing legal advice or legal services to the Government of Manitoba or the **public body**;

Clause 37(1)(i) allows a **public body** to collect **personal information** from a source other than the individual the information is about if the information is collected for use in providing legal advice or legal services to the Government of Manitoba or the **public body**.

Clause 37(1)(i) recognizes that legal counsel representing a **public body** or the Government of Manitoba, and those assisting counsel, may, either in the day-to-day provision of legal advice or legal services or in the provision of legal advice or services respecting legal proceedings, need to collect **personal information** from sources other than the person the information is about. In some circumstances, attempts by legal counsel to collect information directly from the individual the information is about may result in information being withheld or destroyed or in inaccurate information being provided, or the individual may not have the information necessary.

Clause 37(1)(i) applies where:

- the legal advice or legal services are provided to the **public body** that collects the **personal information**, or on whose behalf the **personal information** is collected; or

- where the legal advice or legal services are provided to the Government of Manitoba, in the broad, 'corporate' sense.

The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[108] and is a broader concept than **"department"** or **public body**. Usually, legal proceedings involving a government **department** or **departments** are brought against "The Government of Manitoba" and not against individual **departments**.[109]

The **personal information** may be collected:

- by the **public body** concerned;
- by legal counsel acting for (on behalf of) the **public body** or the Government (including Crown Counsel or Crown Prosecutors in Manitoba Justice; legal counsel on the staff of a **public body**; private bar legal counsel retained by the **public body** or the Government; etc.); or
- by persons assisting legal counsel in providing the legal advice or legal services (including experts, investigators, etc.).

There is some overlap between clause 37(1)(i) and clause 37(1)(h) – indirect collection for legal proceedings.

[108] *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act,* C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

[109] *The Proceedings Against the Crown Act*, C.C.S.M. c. P140, found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p140e.php.

■ History, Release or Supervision of an Individual in Custody, or Security of a Correctional Institution – [Clause 37(1)(j)]

Manner of collection

37(1) **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless

(j) the information concerns

(i) the history, release or supervision of an individual in the custody of or under the control or supervision of a correctional authority, or

(ii) the security of a correctional institution;

Clause 37(1)(j) permits collection of **personal information** from a source other than the individual the information is about in two separate circumstances.

(i) The information concerns the history, release or supervision of an individual in the custody or under the control or supervision of a correctional authority – [paragraph 37(1)(j)(i)]

This paragraph permits correctional authorities, and their agents, to obtain certain information about individuals in their custody or under their control or supervision from a variety of sources. Often the individual concerned either will not or cannot provide accurate and complete information.

The information collected must concern (relate to):

- the history (background, etc.);
- the release (including attitudes and behaviour relevant to possible release); or
- the supervision;

of an individual in the custody or under the control or supervision of a correctional authority.

"Custody" may mean actual imprisonment or physical detention or the power, legal or physical, to imprison.[110] Examples of persons who are in the custody of a correctional authority include:

- persons who are detained in custody under a federal or provincial statute or a municipal bylaw;
- persons remanded in custody by a court, who are charged but not yet found guilty or are not yet sentenced;
- young persons detained in open or secure custody, or who are in pre-trial detention, under the *Youth Criminal Justice Act* (Canada);
- parole violators detained in custody under a warrant issued by a parole board.

“Supervision” means having general oversight or superintendence over a person.[111] Adults and young persons who are subject to control by a correctional authority or its agents due to legally imposed restrictions on their liberty are "under the control or supervision of a correctional authority". Examples include:

- persons on parole,
- persons on probation,
- persons on a temporary absence permit,
- persons under bail supervision,
- persons performing community service work under a court order.

[110] *Black’s Law Dictionary, 6th Edition*.

[111] *Black’s Law Dictionary, 6th Edition.*

(ii) The information concerns the security of a correctional institution - [paragraph 37(1)(j)(ii)]

A **public body** may collect **personal information** from a source other than the individual the information is about if the information concerns the security of a correctional institution.

"Correctional institution" means a place of lawful detention; a "custodial facility" under *The Correctional Services Act*.[112]

"Security" generally means a condition of safety from attack or danger[113] or a state of physical integrity.

The security of a correctional institution includes the safety of the occupants as well as the integrity of the physical structure and the security of adjoining or connecting structures.

[112] *The Correctional Services Act*, C.C.S.M. c. C230, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/c230e.php.

[113] *The Concise Oxford Dictionary, 9th Edition.*

■ Collected to Enforce a Family Maintenance Order – [Clause 37(1)(k)]

Manner of collection

37(1) **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless

(k) the information is collected for the purpose of enforcing a maintenance order under *The Family Maintenance Act*;

Clause 37(1)(k) authorizes staff of the Maintenance Enforcement Office of Manitoba Justice to collect **personal information** from various sources for the purpose of enforcing an order requiring the payment of maintenance (support) for a child, spouse or former spouse.

Often this information cannot be collected directly from an individual who is 'in default' under a maintenance order as he or she cannot be located or is resisting making the support payments under the order.

This clause complements subsections 55(2) and (2.1) of *The Family Maintenance Act*, which authorize a 'designated officer' under that Act to collect certain information from various sources, including government **departments**, agencies and other persons, respecting:

- the whereabouts of a person who is entitled to receive, or who is required to make, payments under an order for spousal or child maintenance (support);
- the financial means, assets and liabilities of a person required to make payments under a maintenance order; etc.

■ Collected to Inform the Public Guardian and Trustee or the Vulnerable Persons Commissioner – [Clause 37(1)(l)]

Manner of collection

37(1) **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless

(l) the information is collected for the purpose of informing The Public Guardian and Trustee or the Vulnerable Persons Commissioner about clients or potential clients;

1. The Public Guardian and Trustee

The role and responsibilities of the Public Guardian and Trustee are largely set out in *The Public Guardian and Trustee Act* and in *The Mental Health Act* and include:

- acting as the 'committee' (that is, the substitute decision maker) of mentally incompetent persons under the authority of *The Mental Health Act* or an order of the Court of Queen's Bench;
- acting as the substitute decision maker for property or personal care, or both, for adults living with a mental disability, when appointed under *The Vulnerable Persons Living with a Mental Disability Act*;
- consenting to or refusing consent to psychiatric treatment on behalf of mentally incompetent patients in psychiatric facilities who have no one else competent and authorized to make these decisions;
- acting as Official Administrator for the province of Manitoba, which involves acting as administrator of last resort of estates in Manitoba where there is no one willing or able to act;
- acting as Official Guardian for the province of Manitoba;
- acting as the litigation guardian for children under 18 years of age and for mentally incompetent persons who have no one else competent to act on their behalf;

- acting as trustee for funds payable to children under 18 years of age;
- reviewing all settlements involving children under 18 years of age;
- reviewing all applications for private committeeship (that is, applications by private persons to be appointed as another person's substitute decision maker).

2. The Vulnerable Persons Commissioner

The role and responsibilities of the Vulnerable Persons Commissioner are set out in *The Vulnerable Persons Living with a Mental Disability Act*. The primary responsibility of the Commissioner is to appoint substitute decision makers for property, for personal care, or both, for adults who are unable to make decisions about the management of property or personal care on their own because of a mental disability.

3. Information collected to inform the Public Guardian and Trustee or the Vulnerable Persons Commissioner about a client or potential client [clause 37(1)(l)]

Clause 37(1)(l) permits **personal information** about the situation, condition and needs of current and potential clients of the Public Guardian and Trustee or of the Vulnerable Persons Commissioner to be collected from a variety of sources, in order that these officials may properly carry out their responsibilities respecting those clients.

■ Collected to Determine or Verify Eligibility – [Clause 37(1)(m)]

Manner of collection

37(1) **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless

(m) the information is collected for the purpose of

(i) determining the eligibility of an individual to participate in a program of or receive a benefit or service from the Government of Manitoba or the **public body** and is collected in the course of processing an application made by or on behalf of the individual the information is about, or

(ii) verifying the eligibility of an individual who is participating in a program of or receiving a benefit or service from the Government of Manitoba or the **public body**;

Clause 37(1)(m) permits a **public body** to collect **personal information** from sources other than the individual the information is about in two circumstances.

1. Collected to determine eligibility - [Paragraph 37(1)(m)(i)]

Paragraph 37(1)(m)(i) contains two requirements:

(i) the **personal information** must be collected for the purpose of determining the eligibility of an individual to participate in a program of or receive a benefit or service from the Government of Manitoba or the **public body** that is collecting the **personal information**; and

(ii) the **personal information** must be collected in the course of processing an application made by or on behalf of the individual the information is about.

"Determining eligibility" in the context of paragraph 37(1)(m)(i) means determining whether an individual is qualified, fit or entitled[114] to participate in a program of or to receive a benefit or service from the Government of Manitoba or the **public body** collecting the **personal information**.

Many programs, services or benefits provided by the Government of Manitoba or by a **public body** have eligibility criteria that must be met for an individual to qualify to participate in the program or to receive the benefit or service. Paragraph 37(1)(m)(i) recognizes that the **public body** may have to obtain **personal information** from several different sources, as well as from the individual the information is about, to determine if the eligibility criteria have been met.

Determination of eligibility takes place at the point the **public body** considers the initial application to participate in the program or receive the benefit or service. For this reason, paragraph 37(1)(m)(i) authorizes collection of **personal information** from other sources only in the course of processing an application made by the individual the information is about, or by a person authorized to act on his or her behalf.

The program, benefit or service may be one offered by the Government of Manitoba or by the **public body** collecting the **personal information**. The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[115] and is a broader concept than **"department"** or **"public body"**.

Keeping in mind the "Openness" Privacy Principle, if a **public body** intends to rely on paragraph 37(1)(m)(i) in an application process, the **public body** may want to consider notifying applicants that **personal information** will be collected from a variety of sources to determine their eligibility. For example, this notice could be included in the application form for the program, service or benefit.

---

114 *Black's Law Dictionary, 6th Edition; The Concise Oxford Dictionary, 9th Edition*.

115 *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act,* C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

2. Collected to verify eligibility - [Paragraph 37(1)(m)(ii)]

Paragraph 37(1)(m)(ii) permits a **public body** to collect **personal information** from sources other than the individual the information is about if the **public body** is "verifying the eligibility" of the individual who is participating in a program or who is receiving a benefit or service from the Government of Manitoba or the **public body** collecting the information.

To "verify" eligibility in the context of paragraph 37(1)(m)(ii) means to confirm, substantiate, authenticate, check or test[116] the qualifications or entitlement of an individual to participate in or receive, or to continue to participate in or receive, a program, benefit or service from the Government of Manitoba or the **public body**.

In this situation, the individual is already participating in the program or receiving the benefit or service, and the **public body** is checking to confirm that the individual was originally qualified, or continues to be qualified, to do so.

The program, benefit or service may be one offered by the **public body** that is collecting the **personal information** or by the Government of Manitoba. The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[117] and is a broader concept than **"department"** or **"public body"**.

Verification of eligibility may be done on a regular basis, on a random basis or as a result of information received by the **public body**.

Information from other sources may be required to verify eligibility for a number of reasons: the individual may not be able to provide the information or all the information required; he or she may not be willing to provide the information or may provide inaccurate information; etc. In such circumstances, the individual will not usually be informed that verification of eligibility is taking place.

---

116 *Black's Law Dictionary, 6th Edition*.

117 *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act,* C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

■ Determining or Collecting a Fine, Debt, Tax or Payment Owing or Making a Payment – [Clause 37(1)(n)]

> **Manner of collection**
> **37(1)** **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless
>
> (n) the information is collected for the purpose of
>
> (i) determining the amount of or collecting a fine, debt, tax or payment owing to the Government of Manitoba or the **public body**, or an assignee of either of them, or
>
> (ii) making a payment;

1. Collected to determine the amount of or to collect a fine, debt, tax or payment owing to the Government of Manitoba or the public body, or an assignee of either of them - [Paragraph 37(1)(n)(i)]

If a **public body** needs to determine the amount of, or to collect, a fine, debt, tax or payment owing to it or to the Government of Manitoba, paragraph 37(1)(m)(i) allows the **public body** to collect the necessary **personal information** from sources other than the individual the information is about. This may be necessary if the **public body** cannot locate the individual, believes it would not obtain complete or accurate information from the individual, etc.

"Determining" the amount of a fine, debt, tax or payment owing means finding out or establishing[118] that amount.

"Collecting" a fine, debt, tax or payment owing occurs once a decision has been made by the **public body** that the individual owes the fine, debt, tax or payment and the **public body** intends to seek payment of the amount owing.

---

[118] *The Concise Oxford Dictionary, 9th Edition*.

A "fine" is a sum of money ordered to be paid to the Government of Manitoba by an offender, as punishment for an offence.[119]

A "debt" is a specified amount of money due to the Government of Manitoba or to the **public body** collecting the **personal information**, and includes not only the obligation of the debtor to pay but also the right of the creditor to receive and enforce the payment.[120]

A "tax" is "a contribution to state revenue compulsorily levied on individuals, property or businesses" [121] and includes federal, provincial, municipal and school taxes.

The phrase "payment owing" is broad and includes amounts that are payable to the Government of Manitoba or to the **public body** collecting the **personal information** – for example, unpaid licence fees, etc.

For paragraph 37(1)(n)(i) to apply, the fine, debt, tax or payment must be:

- owing to the Government of Manitoba.

  The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[122] and is a broader concept than **"department"** or **"public body"**; or

- owing to the **public body** that is collecting the **personal information**, or on whose behalf the **personal information** is collected; or

- owing to an "assignee" of either of them.

  An "assignee" of the Government of Manitoba or of the **public body** is a person to whom the rights of the Government or the **public body** in the fine, debt, tax or payment have been transferred, usually by a written transfer document called an 'assignment'.[123]

---

119 *The Dictionary of Canadian Law.*

120 *The Dictionary of Canadian Law; Black's Law Dictionary, 6th Edition.*

121 *The Concise Oxford Dictionary, 9th Edition.*

122 *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act,* C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

123 *Black's Law Dictionary, 6th Edition*; *The Dictionary of Canadian Law*.

2. Collected to make a payment - [Paragraph 37(1)(n)(ii)]

A “payment” in the context of paragraph 37(1)(n)(ii) is a sum of money that the Government of Manitoba or the **public body** owes to an individual.

Paragraph 37(1)(n)(ii) permits the **public body** to obtain **personal information** from sources other than the individual the information is about "for the purpose of … making a payment". This situation will most commonly arise when a **public body** or the Government of Manitoba owes an individual money and

- the individual has moved and the **public body** does not have a forwarding address; or

- the **public body** is trying to verify the identity of the individual so it can make the payment.

■ Collected to Manage or Administer Personnel – [Clause 37(1)(o)]

> **Manner of collection**
> **37(1)** **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless
>
> (o) the information is collected for the purpose of managing or administering personnel of the Government of Manitoba or the **public body**;

To "manage" means to organize, regulate, be in charge of.[124]

To "administer" means to attend to the running of (business affairs, etc.); manage; be responsible for the implementation of.[125]

"Personnel" means a body of employees.[126]

The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[127] and is a broader concept than **"department"** or **"public body"**.

"Managing or administering personnel" in the context of clause 37(1)(o) includes all aspects of the internal management and administration of the human resources of a specific **public body** and also includes the government-wide management and administration of government personnel through the Manitoba Civil Service Commission.

---

124 *The Concise Oxford Dictionary, 9th Edition*.

125 *The Concise Oxford Dictionary, 9th Edition*

126 *The Concise Oxford Dictionary, 9th Edition*.

127 *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act,* C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

Management of personnel refers to aspects of the management of personnel of a **public body** or the Government of Manitoba that relate to the duties and responsibilities of employees.[128] It includes things such as:

- staffing requirements;
- job classification, recruitment and selection;
- salary and benefits;
- hours and conditions of work;
- leave management;
- performance review;
- training;
- termination of employment and lay-off;
- management of personal service contracts of contract employees, etc.

Administration of personnel consists of all aspects of a **public body's** internal management, other than personnel management that are, necessary to support the delivery of programs and services. Administration includes business planning and financial, contracts, property, information and risk management. [129]

"Managing or administering personnel" does not include management of independent contractors and consultants.

Clause 37(1)(o) permits a **public body** to collect **personal information** about its employees from its own personnel files, from the Manitoba Civil Service Commission, or from other sources rather than returning to the individual each time information is needed. But, the information must be necessary for the purpose of carrying out official duties relating to the management or administration of personnel of the **public body** collecting the information or of personnel of the Government of Manitoba.

Also, as is the case with all **personal information** collected by a **public body**, the **public body** must limit the amount of **personal information** collected to only as much information as is "reasonably necessary" to manage or administer its personnel – the "minimum amount necessary" rule in subsection 36(2) of FIPPA.[130]

---

128 See Alberta Information and Privacy Commissioner Investigation Report 2001-IR-006, found at: http://www.oipc.ab.ca/ims/client/upload/2001-IR-006.pdf.

129 See Alberta Information and Privacy Commissioner Investigation Report 2001-IR-006, found at: http://www.oipc.ab.ca/ims/client/upload/2001-IR-006.pdf.

130 Subsection 36(2) of FIPPA is discussed earlier in this Chapter, under *Collection of Personal Information – Limit on Collection*.

While clause 37(1)(o) permits the indirect collection of **personal information** for the purpose of managing or administering personnel, keeping in mind the "Openness" Privacy Principle, a **public body** may want to consider informing its staff, in a general way, of the following:

- how and from what sources personnel information about them is collected;
- the purposes for which the information is used, and by whom; and
- how employees may obtain access to, and request correction of, their **personal information**.

Some **public bodies** may be required to provide this and other information to **employees** under a collective agreement or other contract of employment.

■ Collected to Audit, Monitor or Evaluate Activities – [Clause 37(1)(p)]

> **Manner of collection**
> **37(1)** **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless
>
> (p) the information is collected for the purpose of auditing, monitoring or evaluating the activities of the Government of Manitoba or the **public body**; or

Clause 37(1)(p) permits a **public body** to collect **personal information** from sources other than the individual the information is about if the information is collected for the purpose of:

- auditing, monitoring or evaluating the activities of the Government of Manitoba in the broad, 'corporate' sense.

  The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[131] and is a broader concept than **"department"** or **"public body"**.

- auditing, monitoring or evaluating the **public body's** own activities.

An "audit" is an official examination of accounts or a systematic review[132] of the activities of the Government of Manitoba or of the **public body** collecting the **personal information**.

To "monitor" activities means to check or maintain regular surveillance[133] over the activities of the Government of Manitoba or of the **public body** collecting the **personal information**.

---

131 *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act,* C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

132 *The Concise Oxford Dictionary, 9th Edition.*

133 *The Concise Oxford Dictionary, 9th Edition*.

To "evaluate" activities means to assess or appraise[134] the activities of the Government of Manitoba or of the **public body** collecting the **personal information**.

[134] *The Concise Oxford Dictionary, 9th Edition*.

■ Collected to Determine Suitability for an Honour or Award – [Clause 37(1)(q)]

> **Manner of collection**
> **37(1)** **Personal information** must be collected by or for a **public body** directly from the individual the information is about unless
>
> (q) the information is collected for the purpose of determining suitability for an honour or award, including an honourary degree, scholarship, prize or bursary.

Clause 37(1)(q) permits a **public body** to collect **personal information** from sources other than the individual the information is about for the purpose of determining the individual's suitability for an honour or award.

Clause 37(1)(q) allows a **public body** to collect **personal information** if it is considering bestowing an honour or award on an individual, without the individual's knowledge. The nature of some awards is that the potential recipients do not have to apply for them, and may not be aware they are being considered for them.

Any **personal information** collected should be directly related to the criteria for granting the honour or award. Also, **public bodies** may want to consider making the criteria for an honour or award generally available before collecting **personal information**.

The clause lists some examples of honours or awards **–** an honourary degree, a scholarship, a prize or a bursary – but this is not a complete list as the word "including" is used. Other examples include:

- The Order of the Buffalo Hunt; and
- The Premier's Volunteer Service Award.

■ Information That Must Be Provided to the Individual: The "Privacy Notice" - [Subsections 37(2) and 37(3)][135]

Individual must be informed
37(2) A **public body** that collects **personal information** directly from the individual the information is about shall inform the individual of

(a) the purpose for which the information is collected;

(b) the legal authority for the collection; and

(c) the title, business address and telephone number of an officer or **employee** of the **public body** who can answer the individual's questions about the collection.

When notice not required
37(3) A **public body** need not comply with subsection (2) if it has recently provided the individual with the information referred to in that subsection about the collection of the same or similar **personal information** for the same or a related purpose.

Subsection 37(2) sets out information that a **public body** must provide whenever it collects **personal information** directly from the individual the information is about. This information that a **public body** is required to give to the individual is often referred to as a "privacy notice".

Subsection 37(2) reflects the privacy principles of 'Identifying Purposes' and 'Openness'. 'Openness' is of particular importance, as 'information privacy' is about an individual's control over his or her **personal information**.

[135] A trustee, including a **public body**, that collects **personal health information** directly from the individual it is about must give the individual information about the trustee's collection practices as set out in section 15 of *The Personal Health Information Act*. *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

The requirement in subsection 37(2) that **public bodies** provide certain information to an individual when collecting **personal information** directly from him or her is intended to ensure that an individual is aware of the purpose for which the **personal information** is being collected and how it will be used. This allows the individual to make an informed decision as to whether or not to give the **personal information** to the **public body** in situations where there is no statute or regulation requiring that it be given, and to understand any consequences that may result from not providing the information. Also, to exercise privacy rights under Part 3 of FIPPA, such as the right to complain if the information is being collected, used or disclosed in a manner not authorized by FIPPA, an individual must have some idea of the purpose for which his or her information is being collected.

Remember:

A **public body** can only collect **personal information** if it is authorized to do so under subsection 36(1) of FIPPA. In order to determine if the collection is authorized under FIPPA, the purposes for which the **personal information** is being collected must first be identified.

1. What information must be provided to the individual

Subsection 37(2) requires that, when a **public body** collects **personal information** directly from the individual the information is about, the **public body** must inform the individual of three things:

(i) The purpose for which the public body is collecting the information.

The "purpose" for collecting the information is the reason why the **public body** needs the **personal information**, and how it intends to use it.

The **personal information** must be collected for a purpose that is authorized under subsection 36(1) of FIPPA.

(ii) The legal authority for collecting the information.

The "legal authority" for collecting the information is the clause in subsection 36(1) of FIPPA – clause 36(1)(a), (b) or (c) – that is being relied on. Also,

- where the **public body** is relying on clause 36(1)(a) of FIPPA – collection is authorized by or under another statute or regulation of Manitoba or Canada – the privacy notice should refer to clause 36(1)(a) of FIPPA and to the specific provision in the other Act or regulation that authorizes the collection;

- where the **public body** is relying on clause 36(1)(b) of FIPPA – information relates directly to and is necessary for an existing service, program or activity – the privacy notice should:

    - state that the **public body** is relying on clause 36(1)(b),

    - clearly identify the service, program or activity concerned, and

    - state why the collection of the information is necessary for this purpose.

*(iii) The title, business address and telephone number of an officer or **employee** of the **public body** who can answer the individual's questions about the collection.*

The **public body** should provide the individual with a knowledgeable contact who is familiar with the service, program or activity for which the **personal information** is being collected, and who can explain why the **personal information** is being collected, how it will be used and disclosed, etc.

2. Circumstances in which the privacy notice must be given

The privacy notice required in subsection 37(2) must be given whenever the **public body** is collecting **personal information** directly from the individual the information is about.

The **public body** should endeavour to inform the individual about the matters set out in subsection 37(2) at the time the **personal information** is collected from him or her.

If a **public body** has recently provided the individual with the privacy notice about the collection of the same or similar **personal information** for the same or a related purpose, the **public body** is not required to provide this information again [subsection 37(3)].

3. Form of privacy notice

Subsection 37(2) sets out the required contents of the privacy notice, but does not require that the notice be in a particular form or specify how the required information must be given.

The form of the notice should be appropriate to the situation. Whenever reasonable, the privacy notice should be given in writing – for example, on an application form, on a separate sheet, in a brochure given to the individual, on a poster, etc.

Public bodies should review application forms and other forms and documents used to collect **personal information** to ensure that the required privacy notice is included. A sample privacy notice can be found in the *Model Response Letters and Notices*, on the FIPPA website at: http://www.gov.mb.ca/chc/fippa/public_bodies/resources_public_bodies.html.

Also, the Ombudsman has provided sample wording in the Ombudsman Practice Note: *Collecting and Providing Notice of Collection of Personal Information under FIPPA*.[136]

If there are any questions about appropriate wording, contact the Information and Privacy Policy Secretariat of Manitoba Sport, Culture and Heritage, or legal counsel.

In some circumstances, it may be more practical and effective to provide the required notice verbally – for example:

- if information is collected over the telephone,

[136] This Ombudsman Practice Note can be found on the Ombudsman's website at: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

- if the individual has difficulty understanding written information,
- if information is being gathered in the course of an investigation into a **law enforcement** matter, etc.

If the required privacy notice is given verbally, the officer or **employee** of the **public body** giving the notice should keep a written record of the information provided. The **public body** should also consider whether it is practical and advisable to follow-up a verbal notice of privacy rights with written confirmation or a written privacy notice.

Regardless of the form and manner in which the privacy notice is given – whether in writing or orally – all the required information (purpose, legal authority and contact information) must be provided.

Note: The Privacy Notice and Consent

Giving the required privacy notice should not be confused with obtaining a consent.

The purpose of a privacy notice is to inform the individual – to give him or her information – about the purposes and legal authority for the collection of his or her **personal information** and to provide a contact who can give the individual more information (answer questions, etc.). A privacy notice is a legal requirement – it must be given – but it does not authorize the **public body** to do anything.

The purpose of a consent is very different. A valid consent authorizes (permits) the **public body** to do something (e.g. to disclose **personal information**, etc.). To be valid, a consent must (amongst other things) be 'informed' – that is, it must be based on accurate and relevant information given by the **public body**, including the information given in a privacy notice.[137]

[137] Consent is discussed earlier in this Chapter, under *Consent and FIPPA*.

ACCURACY OF PERSONAL INFORMATION - [SECTION 38][138]

Accuracy of personal information

38 If **personal information** about an individual will be used by a **public body** to make a decision that directly affects the individual, the **public body** shall take reasonable steps to ensure that the information is accurate and complete.

Section 38 of FIPPA reflects the 'Accuracy' privacy principle. It requires a **public body** to "take reasonable steps" to ensure that **personal information** is accurate and complete if that **personal information** will be used by the **public body** to make a decision that "directly affects" the individual the information is about.

"Accurate" means careful, precise, lacking errors.

"Complete" means without omissions or deficiencies.

1. "A decision that directly affects" the individual

The accuracy and completeness requirement in section 38 applies where the **public body** will use the **personal information** to "make a decision that directly affects the individual" the information is about.

A "decision that directly affects" an individual is a decision that has an impact on the individual's life or on his or her rights. This phrase is very broad. Examples of decisions that directly affect an individual include determining whether or not the individual is entitled to a benefit such as social assistance or a student loan, is eligible for a service such as training, is suitable for employment by the **public body**, etc.

The requirement in section 38 does not apply if **personal information** is not used or intended to be used to make a decision, adverse or otherwise, about the individual.

---

[138] Section 16 of *The Personal Health Information Act* requires that a trustee, including a **public body**, take reasonable steps to ensure that **personal health information** is accurate, up to date, complete and not misleading before using or disclosing the information. *The Personal Health Information Act, C.C.S.M. c. P33.5,* can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

2. "Reasonable steps" to ensure accuracy or completeness

"Reasonable" means fair, proper, suitable under the circumstances.[139]

"Reasonable steps" are steps that a fair and rational person would expect to be taken or would find acceptable. The "reasonable steps" to be taken by a **public body** to ensure **personal information** is accurate and complete will depend on the specific circumstances.

"Reasonable steps" will include verifying the accuracy of the information – that is, checking the information for accuracy, including errors and omissions – at the time the **personal information** is collected. The means used to verify **personal information** at the time it is collected (for example, production of supporting documents such as a birth certificate) should be recorded.

To maintain accuracy and completeness of **personal information**, a **public body** will want to consider measures such as

- implementing procedures to update **personal information** that is used on a regular or continuous basis;
- periodically auditing files, with accuracy and completeness as one of the criteria tested;
- ensuring limited access to the **personal information** for the purpose of making corrections or changes;
- establishing cross**–**referencing and validation checks; etc.

Before **personal information** is used in making a decision affecting the individual it is about, the following questions may be helpful in assessing its accuracy and completeness.

- Was the **personal information** collected directly from the individual it is about?

[139] *Black's Law Dictionary, 6th Edition*.

Was the accuracy of the **personal information** verified at the time it was collected?

- Is the proposed use of the **personal information** consistent with the purpose for which it was collected?

- What is the likelihood that the **personal information** is outdated? How old is the information? Is it likely that circumstances have changed since the information was collected?

- Are there systems in place to check the accuracy and completeness of the **personal information –** for example, periodic audits of files for accuracy, cross**-**referencing to other related files, systematic procedures for updating **personal information**, etc.?

REQUESTS TO CORRECT PERSONAL INFORMATION - [SECTION 39][140]

Section 39 of FIPPA reflects one aspect of the 'Access to and Correcting One's Own Personal Information' privacy principle, and one of the stated purposes of FIPPA – "to allow individuals a right to request corrections to **records** containing **personal information** about themselves in the custody or under the control of **public bodies**" [clause 2(c) of FIPPA].[141]

■ Overview of "Requests to Correct Personal Information" - [Section 39]

Section 39 of FIPPA:

- gives an individual who has been given access to a **record** containing his or her **personal information** under Part 2 of FIPPA the right to ask the **public body** to correct **personal information** in the **record** if it is wrong or incomplete;

- requires the **public body** to add the request for correction to the **record** if the **public body** refuses to correct the **record**;

- gives the individual the right to complain to the **Ombudsman** about a **public body's** refusal to correct the **record**; and

- requires the **public body**, where practicable, to notify other **public bodies** or **third parties** who have received the **personal information** from it within the previous year of the correction or request for correction, so they can update their records.

---

[140] Section 12 of *The Personal Health Information Act* deals with requests to correct **personal health information**. These provisions are similar to the provisions of section 39 of FIPPA. *The Personal Health Information Act, C.C.S.M. c. P33.5,* can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

[141] The privacy principles on which FIPPA is based are discussed earlier in this Chapter, under *The Privacy Principles in FIPPA*. Clause 2(c) and the other purposes in section 2 of FIPPA are discussed in Chapter 1, under *Purposes of FIPPA*.

Note:

Not all requests to correct **personal information** need to be, nor indeed should be, made under section 39 of FIPPA.

Section 39 does not replace existing procedures under which an individual can request correction of **personal information** in a **record**. Nor does section 39 prevent a **public body** from correcting **personal information** that is clearly incorrect or out of date. Indeed, if the **public body** uses the personal information to make a decision that directly affects the individual the information is about the **public body** has a duty to take reasonable steps to ensure that the information is "accurate and complete" under section 38 of FIPPA.

The formal procedures in section 39 of FIPPA will ordinarily only come into play where there is a dispute between the individual and the **public body** about the accuracy or completeness of the **personal information** in a **record**.

How to Request Correction of Personal Information - [Subsections 39(1) and 39(2)]

Right to request correction
39(1) An **applicant** who has been given access to a **record** containing his or her **personal information** under Part 2 and who believes there is an error or omission in the information may request the **head** of the **public body** that has the information in its custody or under its control to correct the information.

Written request
39(2) A request must be in writing.

A request to correct an "error or omission" in **personal information** in a **record** can only be made under subsection 39(1) of FIPPA by or on behalf of an individual who has applied for and been given access to a **record** containing **personal information** about himself or herself under Part 2 of FIPPA – Access to Information.

An "error" is incorrect, mistaken or wrong information.[142] An "omission" is something that has been overlooked or left out or that is missing.[143]

A request under FIPPA to correct an error or omission in **personal information** must be made in writing to the **public body** that has the **personal information** in its custody or under its control. But, there is no required form for a request for correction of **personal information**.

In most cases, "custody" of a **record** for the purposes of FIPPA means having physical possession of the **record** and "control" of a **record** means having the authority or power to make decisions about the use or disposition of the **record**.[144]

142 *The Concise Oxford Dictionary, 9th Edition*.

143 *The Concise Oxford Dictionary, 9th Edition*.

144 The terms "custody" and "control" are discussed in Chapter 2, under *Custody or Control of a Record*.

■ Time Limit for a Decision about Correction - [Subsections 39(3) and 39(4)]

Head's response
39(3) Within 30 days after receiving a request under subsection (1), the **head** of the **public body** shall.....

Extended time limit
39(4) Subsection 15(1) applies with necessary modifications to the period set out in subsection (3).

The **head** of the **public body** (or his or her delegate under section 81 of FIPPA)[145] must make a decision about a request to correct **personal information** within 30 days after receiving the written request.

This time period can be extended for up to 30 additional days, or longer if the Ombudsman agrees, for the reasons set out in subsection 15(1) of FIPPA (as adapted to make these reasons apply to requests to correct **personal information**).

That is, the 30 day time limit for responding to a request to correct **personal information** may be extended if:

(a) the person requesting does not give enough detail to enable the **public body** to identify the **record** to be corrected;

(b) the person is requesting that a large number of **records** be corrected or a large number of **records** must be searched, and responding within the 30 day time limit would interfere unreasonably with the operations of the **public body**;

(c) time is needed to consult with a **third party** or another **public body** before deciding whether or not to correct the **record**.

[145] Delegation by the head of a public body of powers and duties under FIPPA is discussed in Chapter 3, under *Roles and Responsibilities of Public Body Officials*.

■ Decision about Request to Correct Information - [Subsection 39(3)]

Head's response
39(3) Within 30 days after receiving a request under subsection (1), the **head** of the **public body** shall

(a) make the requested correction and notify the **applicant** of the correction; or

(b) notify the **applicant** of the **head's** refusal to correct the **record** and the reason for the refusal, that the request for correction has been added to the **record**, and that the individual has a right to make a **complaint** about the refusal under Part 5.

The **head** of the **public body** (or his or her delegate under section 81 of FIPPA) may do either of (a) or (b):

(a) make the requested correction and notify the individual who made the request of the correction;

A **public body** may occasionally 'correct' a **record** by physically changing the **record** to erase the original, incorrect, information. More commonly, however, a **public body** will correct a **record** by clearly marking the original information as incorrect and attaching the correct information to the **record**.

(b) refuse to make the requested correction, in which case the **head** must:

(i) add the request for correction to the **record**; and

(ii) notify the individual who made the request:

- of the refusal to correct the **record** and the reason for the refusal;
- that the request for correction has been added to the **record**; and

- that the individual has a right to make a **complaint** to the **Ombudsman** about the refusal to correct the **record** under Part 5 of FIPPA.[146]

A **public body** may refuse, or be unable, to make a requested correction to a **record** because, for example:

- in the case of an alleged factual error, the person requesting the correction has not submitted adequate proof in support of the requested correction;

- the information is non-factual evaluative information or an opinion, and the **applicant** and the **public body** hold differing views or opinions. If the **applicant** does not agree with an opinion, he or she may have the request for correction attached to the opinion but the **public body** cannot be required to change the opinion stated.[147]

The **public body** must add the request for correction to the **record** in a way that ensures that the request is always retrieved with the original information.

[146] Complaints under FIPPA are discussed in Chapter 8 of this Manual.

[147] Ontario Information and Privacy Commissioner Order P-321 (Re Ministry of Correctional Services), June 24, 1992.

■ Duty to Notify Others - [Subsections 39(5) and 39(6)]

Notice to others

39(5) On correcting a **record** or adding a request for correction to a **record** under this section, the **head** of the **public body** shall, where practicable, notify any other **public body** or **third party** to whom the information has been disclosed during the year before the correction was requested that the correction has been made or a request for correction has been added.

Correction required

39(6) On being notified under subsection (5) of a correction or request for correction, a **public body** must make the correction or add the request for correction to any **record** of that information in its custody or under its control.

Subsection 39(5) requires that, "where practicable", a **public body** that has corrected a **record** or added a request for correction to a **record** under subsection 39(4) must notify other **public bodies** and **third parties**, to which it has disclosed this **personal information** during the year prior to the request for correction, of the correction or request for correction so these bodies can update their records.

A **public body** "discloses" **personal information** any time it makes the information known to, or reveals, exposes,[148] shows, provides or sells **personal information** to, or shares the information with, any person or entity outside the **public body** by any means (for example, by providing copies, electronically or by any other means). Sharing of **personal information** by one Manitoba government **department** with another **department** is a disclosure of **personal information** for the purposes of FIPPA, as each **department** is a separate **public body**.

"Where practicable" means that the correction or request for correction must be provided except where it is not reasonably possible to do so.

In order for a **public body** to be able to comply with this duty to notify other **public bodies** and **third parties** of corrections or requests for corrections, the **public body** will need to keep records of any disclosures of **personal information** to other **public bodies** and **third parties**.

[148] *The Concise Oxford Dictionary, 9th Edition*; *Black's Law Dictionary, 6th Edition*.

Subsection 39(6) requires that, if a **public body** receives notice of correction or of a request for correction from another **public body,** it must either make the correction to its own **record** of the **personal information** or add the request for correction to its **record**. This must be done in a way that ensures that the correction or request is always retrieved with the original information.

Also see Ombudsman Practice Note: *Handling Requests for Correction under FIPPA*.[149]

[149] This Practice Note can be found on the Ombudsman's website at: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

RETENTION OF PERSONAL INFORMATION - [SECTION 40]
[150]

Retention of personal information
40(1) A **public body** that uses **personal information** about an individual to make a decision that directly affects the individual shall, in the absence of another legal requirement to do so, establish and comply with a written policy concerning the retention of the **personal information**.

Content of retention policy
40(2) A policy under subsection (1) must

(a) require that **personal information** be retained for a reasonable period of time so that the individual the information is about has a reasonable opportunity to obtain access to it; and

(b) comply with any additional requirements set out in the regulations.

1. Meaning of "Retention"

The term "retention" is not defined in FIPPA. In general, to "retain" **personal information** means to continue to hold, have or keep the **personal information**.[151]

2. When is a public body required to establish a records retention policy under FIPPA? [Subsection 40(1)]

The requirement to establish a written retention policy under subsection 40(1) of FIPPA only applies "in the absence of another legal requirement to do so". For example, this requirement does not apply if the retention of **records** by the **public body** is addressed in another statute or in a regulation.

---

[150] Section 17 of *The Personal Health Information Act* deals with retention and destruction of **personal health information**. *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

[151] *Black's Law Dictionary, 6th Edition*.

In the case of all Manitoba government **departments** and certain **government agencies**, retention and destruction of **records**, including **records** of **personal information**, are governed by *The Archives and Recordkeeping Act* and the Records Schedules approved under that Act. Government **departments** and those **government agencies** that fall under *The Archives and Recordkeeping Act* and that have (and comply with) approved records schedules under *The Archives and Recordkeeping Act* are not required to have a separate retention policy for **records** containing **personal information**.[152]

Those **public bodies** that do not fall under *The Archives and Recordkeeping Act* or other legislation respecting the retention of records must establish a written retention policy respecting **personal information** that will be used to "make a decision that directly affects the individual" the information is about.

A "decision that directly affects" an individual is a decision that has an impact on the individual's life or on his or her rights. Examples include determining whether or not an individual is entitled to a benefit, is eligible for a service, is suitable for employment by the **public body**, etc.

The requirement in subsection 40(1) does not apply where **personal information** is not used or intended to be used to make a decision, adverse or otherwise, with respect to the individual.

3. Content of retention policy [Subsection 40(2)]

Where a **public body** is required to establish a written retention policy under subsection 40(1) of FIPPA, subsection 40(2) sets out minimum requirements for the policy:

(a) The policy must require that **personal information** be retained for a reasonable period of time so that the individual the information is about has a reasonable opportunity to obtain access to it [clause 40(2)].

> A "reasonable period of time" is a period of time that is fair and appropriate in the circumstances. In this context, a "reasonable" period for retaining or keeping **personal information** is one that is long enough to give the individual the **personal information** is about a fair opportunity to obtain access to his or her information.

(b) The policy must also be consistent with any additional requirements set out

[152] *The Archives and Recordkeeping Act*, C.C.S.M. c. A132, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/a132e.php.

in the regulations made under FIPPA [clause 40(2)(b)].

At present, there are no requirements respecting retention of **personal information** in the *Access and Privacy Regulation* made under FIPPA.[153]

Note:

When a government **department** is establishing a **records schedule** under *The Archives and Recordkeeping Act*, the **department** should consider the requirement in clause 40(2)(a) of FIPPA when determining the appropriate retention period for **personal information**. That is, **personal information** should be retained "for a reasonable period of time so that the individual the information is about has a reasonable opportunity to obtain access to it".

4. Storage and destruction of records containing personal information

Clause 3(b) of FIPPA states that FIPPA:

> does not prohibit the transfer, storage or destruction of any **record** in accordance with any other **enactment** of Manitoba or Canada or a by–law or resolution of a **government agency** or **local public body**.

That is, FIPPA – including section 40 of FIPPA – does not prevent a **public body** from transferring **records** containing **personal information** to, or storing them in, another location, as long as the **public body** can readily retrieve the **records** in order to respond to a request for access under Part 2 of FIPPA.

Nor does section 40 of FIPPA prevent a **public body** from destroying a **record** containing **personal information** if this is done in accordance with:

- a statute or regulation of Manitoba, such as *The Archives and Recordkeeping Act*;
- a statute or regulation of Canada; or
- a by-law or resolution of a **government agency** or of a **local public body**.

[153] A consolidated version of the *Access and Privacy Regulation*, Manitoba Regulation 64/98, as amended, can be found at: http://web2.gov.mb.ca/laws/regs/pdf/f175-064.98.pdf.

If a **public body** hires a contractor or agent to store its **records**, there should be a written contract in place to ensure that **personal information** is properly protected. The contract should address matters such as retrieval of the **records** by the **public body** and use, protection, retention and disclosure of the **personal information** held by the storage agent or organization, etc. Also, the **public body** continues to be responsible for the **personal information** – see the discussion earlier in this Chapter under *Accountability, Employees, Contractors and Agents*.

Legal counsel should be consulted when drafting and negotiating contracts, agreements and arrangements respecting the storage of **records**, especially when the **records** contain **personal information**.

PROTECTION OF PERSONAL INFORMATION - [SECTION 41][154]

Two privacy principles – 'Accountability' and 'Security (Safeguarding Personal Information)' – are reflected in section 41 of FIPPA.

> **Protection of personal information**
> **41** The **head** of a **public body** shall, in accordance with any requirements set out in the regulations, protect **personal information** by making reasonable security arrangements against such risks as unauthorized access, use, disclosure or destruction.

■ Overview of the Duty to Protect Personal Information - [Section 41]

Collecting **personal information** carries with it the duty to protect the **personal information**.

Each **public body** must protect the **personal information** in its custody or under its control by making "reasonable security arrangements" against "such risks as unauthorized access, use, disclosure or destruction". Such arrangements include adopting reasonable physical, administrative and procedural, and technical safeguards for the **personal information**. In determining what safeguards are "reasonable", the **public body** needs to take into account the sensitivity of the **personal information**.

[154] Sections 18 and 19 of *The Personal Health Information Act* and the *Personal Health Information Regulation* (as amended) under that Act set out the security safeguards which a trustee, including a **public body**, is required to take with respect to personal health information and are more detailed than section 44 of FIPPA. *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php. The *Personal Health Information Regulation*, Man. Reg. 245/97, as amended, can be found at: http://web2.gov.mb.ca/laws/regs/pdf/p033-5-245.97.pdf.

The **public body** is responsible for all **personal information** in its custody or under its control. That is, the **public body** must take reasonable steps to ensure that its **employees** – its officers, staff, contractors and agents – comply with the duty to protect **personal information**.[155]

[155] A public body's responsibility for its officers, staff, contractors and agents is discussed earlier in this Chapter, under *Accountability and Employees, Contractors and Agents*.

■ Duty to Protect Personal Information - [Section 41]

At present, there are no specific requirements respecting protection of **personal information** in the *Access and Privacy Regulation* made under FIPPA.[156]

However, **public bodies** need to be aware of the specific security requirements respecting **personal health information** in the *Personal Health Information Regulation* (as amended)[157] under *The Personal Health Information Act*, as these requirements apply to any **personal health information** in their custody or under their control.

1. Custody or control

Collecting **personal information** carries with it the duty to protect the information. Thus, each **public body** is required to protect **personal information** in its custody or under its control.

In most cases, a **public body** will have 'custody' of **personal information** for the purposes of FIPPA when it has physical possession of the **personal information**. **Personal information** is under the 'control' of a **public body** if the **public body** has the power or authority to make decisions about the **personal information**; to manage the **personal information**, including restricting, regulating and administering its use, disclosure or disposition.[158]

A **public body** cannot avoid its responsibility under FIPPA to protect **personal information** by, for example, contracting with an organization to handle the information. The **public body** is responsible for the actions of its contractors and agents, as well as for the actions of its officers and staff. To make this clear, the definition of **"employee"** in subsection 1(1) of FIPPA was amended to include not only officers and employees, but also any person "who performs services for the **public body** under a contract or agency relationship with the **public body**."[159]

---

156 A consolidated version of the *Access and Privacy Regulation*, Man. Reg. 64/98, as amended, can be found at: http://web2.gov.mb.ca/laws/regs/pdf/f175-064.98.pdf.

157 A consolidated version of the *Personal Health Information Regulation*, Man. Reg. 245/97, as amended, can be found at: http://web2.gov.mb.ca/laws/regs/pdf/p033-5-245.97.pdf.

158 The terms 'custody' and 'control' are discussed in Chapter 2, under *Records that Fall Under FIPPA*.

159 Subsection 1(1) of FIPPA. The definition of "employee" was amended by *The Freedom of Information and Protection of Privacy Amendment Act*, S.M. 2008 c. 40. The amending Act can be found at: http://web2.gov.mb.ca/laws/statutes/2008/c04008e.php.

That is, a **public body's** duty to protect **personal information** includes the duty to take reasonable steps to ensure that others who act on its behalf – officers, staff, contractors and agents – also comply with this duty. In the case of contractors and agents, "reasonable steps" will include contractual measures, as well as other measures.[160]

2. "Reasonable security arrangements"

A **public body** is required to protect **personal information** in its custody or under its control from risks such as unauthorized access, use, disclosure or destruction by making "reasonable" security arrangements.

"Reasonable" security arrangements are steps taken to protect the **personal information** that are suitable under the circumstances, fit and appropriate to the end in view, rational.[161]

Reasonable security arrangements would take into account:

(i) the sensitivity of the **personal information** to be protected.

The more sensitive the **personal information**, the greater the potential harm to the individual the information is about if unauthorized access, use, disclosure or destruction occurs; and

(ii) the medium in which the information is stored, handled, transmitted or transferred (for example, paper, tapes, electronically, etc.).

3. " Unauthorized access"

"Unauthorized access" to **personal information** occurs when an **employee** – that is, an officer, staff person, contractor or agent – of a **public body** has access

(i) to **personal information** that he or she does not need to see or handle in the course of carrying out his or her duties; or

---

160 Discussed earlier in this Chapter, under *Accountability and Employees, Contractors and Agents*.

161 *Black's Law Dictionary, 6th Edition*.

(ii) to more **personal information** than he or she needs to carry out these duties.

Subsections 42(2) and (3) of FIPPA state:

> **Limit on amount of information used or disclosed**
> **42(2)** Every use and disclosure by a **public body** of **personal information** must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed.
>
> **Limit on employees**
> **42(3)** A **public body** shall limit the use of **personal information** in its custody or under its control to those of its **employees** 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 43.

"Unauthorized access" also occurs when persons outside the **public body** gain access to **personal information** about other individuals to which they have no right through improper, inadvertent or accidental disclosure or surreptitious means.

4. " Unauthorized use"

"Unauthorized use" of **personal information** occurs when the information is used, dealt with or employed[162] for a purpose that is not permitted under section 43 of FIPPA.

A **public body** is responsible for ensuring that **personal information** is used by its officers, staff, contractors and agents only for the purposes that are permitted in section 43.[163] Section 43 is discussed in detail later in this Chapter, under *Use of Personal Information*.

5. "Unauthorized disclosure""

Unauthorized disclosure occurs when **personal information** is made known, revealed, exposed,164 shown, provided, sold, shared or given in circumstances not permitted under subsection 44(1) of FIPPA.

A **public body** is responsible for ensuring that all disclosures of **personal information** are authorized (permitted) under subsection 44(1) of FIPPA. Section 44 is discussed in detail later in this Chapter, under Disclosure of **Personal Information**.

Example:

If a person applies under Part 2 of FIPPA – Access to Information – for access to a **record** containing **personal information** about someone else, the **public body** must refuse access if disclosure of the **personal information** would be an unreasonable invasion of the privacy of that other person under section 17 of FIPPA. Providing access in this situation would be an "unauthorized disclosure" of **personal information**.[165]

---

162 *Black's Law Dictionary, 6th Edition*.

163 Section 5 of the *Personal Health Information Regulation*, made under *The Personal Health Information Act*, requires that a trustee, including a **public body**, determine the **personal health information** that each of its employees or agents is authorized to have access to. The Consolidated version of the *Personal Health Information Regulation*, 245/97, Man. Reg. as amended, can be found at: http://web2.gov.mb.ca/laws/regs/pdf/p033-5-245.97.pdf.

164 *The Concise Oxford Dictionary, 9th Edition*; *Black's Law Dictionary, 6th Edition*.

165 Section 17 of FIPPA is discussed in Chapter 5 of this Manual.

6. "Unauthorized destruction"

"Unauthorized destruction" occurs when **personal information** is destroyed in a manner that does not comply with applicable legal requirements or approved policies.

In the case of Manitoba government **departments**, and those **government agencies** that fall under *The Archives and Recordkeeping Act*, the Records Schedules approved under *The Archives and Recordkeeping Act* will set out when **records** can be destroyed and the authorized manner of destroying **records**, including r**ecords** containing **personal information**.[166]

7. Determining reasonable security arrangements

A **public body** should analyze:

- the types of **personal information** in its custody or under its control;
- the degree of sensitivity of each type of **personal information**;
- how the information is stored, handled, transmitted or transferred, and the potential risk of unauthorized access, use, disclosure or destruction.

The **public body** should then take steps that are reasonable in the circumstances, including time and resources available, to implement appropriate physical, administrative and procedural, and technical safeguards to protect the **personal information**.

More stringent security measures should be considered for particularly sensitive **personal information** – for example, inmate files, personnel files, etc. Security measures that must be taken with respect to **personal health information** are set out in sections 18 and 19 of *The Personal Health Information Act* and in the *Personal Health Information Regulation* under that Act.[167]

---

[166] Section 17 of *The Personal Health Information Act* deals in detail with destruction of personal health information by trustees, including public bodies. *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

[167] *The Personal Health Information Act, C.C.S.M. c.* P33.5 can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php. The *Personal Health Information Regulation*, Man. Reg. 245/97, as amended, can be found at: http://web2.gov.mb.ca/laws/regs/pdf/p033-5-245.97.pdf.

Note:

The duty to protect **personal information** applies during the whole 'life cycle' of a **record**. For example, **public bodies** must ensure that **personal information** is destroyed in a secure manner that properly protects the privacy of the individual the information is about.

Examples of physical security arrangements include:

- ensuring **personal information** is not left unattended in unsecured areas while being worked on, during transmission or while in interim storage;
- storing **personal information** in locked filing cabinets with controls over distribution of keys or lock combinations or in secure areas where access is limited or restricted;
- labeling file drawers, records storage boxes and other storage containers so as not to reveal the fact that they contain **personal information**; etc.

Examples of administrative and procedural security arrangements include:

- privacy policies and procedures, including security procedures;
- procedures for packaging or transmitting information according to its sensitivity; for example, **personal information** should not be faxed unless reasonable policies and procedures are in place to ensure it will be received by the intended recipient;
- secure disposal procedures for **records** and equipment that take into account the sensitivity of the **personal information** involved;
- a system of authorization and access procedures that limit access to **records** containing **personal information** to authorized employees – officers, staff, contractors and agents – who need to know this information to carry out their duties, as required by subsection 42(3) of FIPPA, including file check out procedures incorporating user security levels; access logs; etc.;

- reference and background checks of officers, staff, contractors and agents to ensure that they are suitable persons to have access to sensitive information, information systems and the facilities in which they are located;

- ensuring that officers and staff understand their responsibilities by providing them with written policies and procedures and training on privacy policies and procedures;

- ensuring that contractors and agents understand and comply with their responsibilities through contractual and other means (including monitoring, etc.);

- procedures for monitoring and reviewing the general effectiveness of, and compliance with, security measures, including periodic audits of access procedures, access logs, etc.;

- establishing sanctions or consequences for contravening security policies and procedures; etc.

Examples of technical security arrangements include:

- using software, hardware or operating system access controls such as passwords that allow different levels of access to various screens and differing capabilities to read, extract or change information based on the need to know; clearance of display screens; transaction logs and error logs;

- using secure communications and encryption, especially if **personal information** is stored on moveable media (e.g. laptops, discs, memory sticks, etc.) and if **personal information** is transmitted electronically;

- automatic auditing or tracking of access and use;

- providing adequate virus protection for new and existing computer equipment;

- restricting the use of less secure forms of communication (e.g. cellular phones);

- conducting audit checks of information and system integrity, and establishing procedures for database recovery and back–up; and

- identifying and implementing other privacy enhancing technologies as appropriate, such as digital signatures;

- ensuring that when equipment such a computers, photocopiers, scanners, etc. are disposed of, all **personal information** is completely and effectively removed or destroyed.

Also see Ombudsman Practice Notes:

- *Protecting Personal and Personal Health Information when Working Outside the Office;*

- *Privacy Considerations for Faxing Personal and Personal Health Information;*

- *Privacy Considerations for Emailing Personal and Personal Health Information*.[168]

A **public body** should consider establishing procedures to regularly monitor security arrangements respecting **personal information** to ensure that appropriate physical, administrative and procedural, and technical security measures are in place and remain at appropriate levels.

Where **personal health information** is concerned, a **public body** is required to audit its security safeguards at least every two years and to take steps to correct any deficiencies identified by the audit as soon as practicable.[169]

---

168 These Practice Notes can be found on the Ombudsman's website at: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

169 Section 8 of the *Personal Health Information Regulation*, under *The Personal Health Information Act*. The *Personal Health Information Regulation*, Man. Reg. 245/97, can be found at: http://web2.gov.mb.ca/laws/regs/pdf/p033-5-245.97.pdf.

Privacy and security measures should not be seen as barriers to applying new technology. Rather, they are essential components of modern information management systems – necessary to maintain public confidence in the use of technology. When developing services, programs and activities, and the systems that support them, **public bodies** need to take into account the privacy rights of individuals and the duty of **public bodies** to protect **personal information** under FIPPA and **personal health information** under *The Personal Health Information Act*. This applies to all aspects of information management, including collection or compilation; controls on accuracy, use, retention and disclosure; protection; and disposal. Privacy requirements should be built in at the earliest stages to ensure that legal and policy requirements are met. Wherever possible, privacy enhancing technologies should be incorporated.

To ensure that privacy protection requirements are taken into account when a service, program or activity is being developed or modified, or when new technologies are being considered, a **public body** should consider carrying out a "privacy impact assessment". Indeed, in some situations, there may be a policy requirement to do so. Privacy Impact Assessments are discussed later in this Chapter.

A Note on the Duty to Protect the Privacy of Access Applicants

The duty in section 41 of FIPPA to protect **personal information** from unauthorized access, use or disclosure applies to any **personal information** that is obtained or collected in the course of receiving and handling a request for access to a **record** under Part 2 of FIPPA – Access to Information.

For example, the name and other identifying information (e.g. home address and home phone number) of an individual making an access request under Part 2 of FIPPA (an "access **applicant**") is **personal information**, and the **public body** receiving the access request must protect this **personal information** in accordance with section 41 of FIPPA. This means that:

- When sharing information about the access request with others in the **public body**:
    - the identity and any other **personal information** provided by the access **applicant** must only be shared with those in the **public body** who need to know the information in order to process the access request or to make a decision about it [subsection 42(3) of FIPPA]; and
    - any sharing of personal identifiers and other **personal information** about the access **applicant** must be limited to the minimum amount necessary to process the access request or to make a decision about it [subsection 42(2) of FIPPA].
- The identity and any other **personal information** about the access **applicant** must not be disclosed to an affected **third party** or another **public body** (for example, in the context of consultations about the access request) unless:
    - the disclosure is necessary to process the access request or to make a decision about it; and
    - the disclosure is limited to the minimum amount of **personal information** necessary to process the access request to make a decision about it [subsection 42(2)].[170]

[170] Also discussed in Chapter 4, under *The Duty to Protect the Privacy of an Access Applicant.*

Example:

Under section 16 of FIPPA, a **public body** may transfer an access request to another **public body** (for example, because that other body has custody or control of the **records** requested). The **public body** can transfer the whole access request, including the name and contact information and other **personal information** provided by the access **applicant** on the Application form, to the other **public body** as that other body needs to know this information to process and deal with the access request.

Also see Ombudsman Practice Note: *Protecting the Privacy of Access Requesters.*[171]

[171] This Practice Note can be found on the Ombudsman's website: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

What to Do If a Privacy Breach Occurs

A privacy breach is an incident involving, or that could reasonably be expected to result in, unauthorized access to, or unauthorized use or disclosure of, **personal information**.

A breach may be accidental – for example, a laptop containing **personal information** is lost or stolen, **personal information** is mistakenly faxed or sent to the wrong person, etc. Or it may be intentional.

If a **public body** is faced with a privacy breach, it is strongly recommended that the **public body** consult with legal counsel and that it consider the following Ombudsman Practice Notes:

- *Key Steps in Responding to Privacy Breaches under The Freedom of Information and Protection of Privacy Act (FIPPA) and The Personal Health Information Act (PHIA)*; and

- *Reporting a Privacy Breach to the Manitoba Ombudsman*.[172]

The Information and Privacy Policy Secretariat of Manitoba Sport, Culture and Heritage can also provide assistance in responding to a privacy breach.

A **public body** should include in its privacy and security policies and procedures the procedures to be followed in the event of a breach of security. Such procedures should include:

- how to respond to a security breach – e.g. how to assess and contain the breach; how it is to be investigated; how to assess potential harm and identify measures to reduce potential harm; how to identify measures to prevent further breaches, etc.;

- to whom the breach should be reported and in what circumstances – e.g. officials in the **public body**; the **Ombudsman**, etc.;

- when the individuals whose **personal information** is affected by the breach should be notified, and how this should be done; and

[172] These Ombudsman Practice Notes can be found on the Ombudsman's website at: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

- any administrative or disciplinary sanctions that will apply in the case of a breach – particularly in the case of an intentional breach.

Note:

Any person who willfully discloses **personal information** in contravention of FIPPA is guilty of an offence and is liable on summary conviction by a court to a fine of not more than $50,000.[173]

When developing a privacy breach policy, a **public body** should consult with its privacy experts and advisors, including legal counsel and the Information and Privacy Policy Secretariat of Manitoba Sport, Culture and Heritage. Also, the **public body** should look to the Ombudsman's two Practice Notes about privacy breaches (referred to above) for guidance.

[173] Subsection 85(1) of FIPPA, discussed in Chapter 3, under *Offences and Penalties*.

USE OF PERSONAL INFORMATION - [SECTIONS 42 AND 43][174]

Sections 42 and 43 set out the rules for the use of **personal information** in the custody or under the control of a **public body**.

Three of the Privacy Principles discussed earlier in this Chapter are particularly relevant to the use of **personal information** by or on behalf of **public bodies**, and are reflected in sections 42 and 43 of FIPPA:

- Accountability;
- Identifying Purposes; and
- Use, Retention and Disclosure Limitation.

[174] Sections 20 and 21 of *The Personal Health Information Act* set out the rules respecting use of **personal health information** by trustees, including **public bodies**. Additional restrictions respecting use of the Personal Health Identification Number, which apply to all persons, not just trustees or **public bodies**, are set out in section 26 of *The Personal Health Information Act*.

Overview of "Use" of Personal Information

Section 42 sets out the limits on the use of **personal information** by **public bodies**. Use of **personal information** must be:

(i) authorized under s. 43 of FIPPA;

(ii) limited to the minimum amount necessary to accomplish the authorized purpose; and

(iii) limited to those **employees** – officers, staff, contractors and agents – who need to know the information to carry out the authorized purposes.

Section 43 sets out the 'authorized uses' – that is, purposes for which a **public body** may use **personal information**.

Reminder: **"personal information"** means "recorded information about an identifiable individual" and includes, but is not limited to, the information listed in clauses (a) to (n) of the definition of this term in subsection 1(1) of FIPPA.[175]

This section of the Manual is broken down as follows:

- the meaning of "use";
- the limits on use of **personal information**;
- authorized uses of **personal information** – general requirements;
- the authorized uses of personal information permitted by clauses 43(a), (b) and (c).

[175] The definition **"personal information"** is discussed in Chapter 2, under *Key Definitions*.

Meaning of "Use"

The term "use" is not defined in FIPPA.

To “use” **personal information** means dealing with or employing[176] **personal information** that is in the custody or under the control of a **public body** by or on behalf of that **public body** to accomplish its objectives.

That is, “use” of **personal information** means access to and use of **personal information** by the officers, staff, contractors and agents of the **public body** with custody or control of the information for the purposes of that **public body**; using or dealing with the **personal information** within or for the purposes of the **public body**.

In most cases, “custody” of a **record** for the purposes of FIPPA means having physical possession of the **record** and “control” of a **record** means having the authority or power to make decisions about the use or disposition of the **record**.[177]

In practical terms:

(i) a **public body** "uses" **personal information** when its officers and staff have access to and use the **personal information** for the purposes of the **public body**.

> This includes situations where **personal information** is shared between the various divisions or programs of the **public body** – the **public body** is “using” the **personal information**;

(ii) a **public body** also "uses" **personal information** when the **personal information** is collected and used by, or is shared with and used by, contractors or agents providing services to the **public body**.

> When a **public body** provides **personal information** to its contractor or agent, this is a "use" of **personal information** by the **public body**, not a "disclosure", as the contractor or agent is receiving and using the **personal information** on behalf of the **public body**. In these circumstances, the contractor or agent is not considered to be separate from the **public body** for the purposes of FIPPA.

---

176 *Black’s Law Dictionary, 6th Edition*.

177 The terms; ‘custody’ and ‘control’ are discussed in Chapter 2, under *Records that Fall Under FIPPA*.

> To make this clear, as of January 1, 2011, the definition of **"employee"** in subsection 1(1) of FIPPA was amended to include not only the officers and staff of a **public body**, but also any person "who performs services for the **public body** under a contract or agency relationship with the **public body**".[178]
>
> But, this also means that a **public body** is responsible for the actions of its contractors and agents.[179]

It is important to note that, under FIPPA, each **department** of the Government of Manitoba is a separate **public body**. For example, when Manitoba Family Services deals with **personal information** within the **department**, it is "using" the **personal information** and the "use" must be authorized under section 43 of FIPPA. But, if Family Services shares the **personal information** with another **department**, such as Education and Advanced Learning, Family Services is "disclosing" the information and the disclosure must be authorized under section 44 of FIPPA. For the purposes of FIPPA, the **departments** of Manitoba Family Services and Manitoba Education and Advanced Learning are separate – they are two distinct **public bodies**.

---

[178] The definition "employee" was amended by *The Freedom of Information and Protection of Privacy Amendment Act*, S.M. 2008 c. 40. The amending Act can be found at: http://web2.gov.mb.ca/laws/statutes/2008/c04008e.php.

[179] Discussed earlier in this Chapter, under *Accountability and Employees, Contractors and Agents*.

■ Limits on Use of Personal Information - [Section 42]

General duty of public bodies
42(1) A **public body** shall not use or disclose **personal information** except as authorized under this Division.

Limit on amount of information used or disclosed
42(2) Every use and disclosure by a **public body** of **personal information** must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed.

Limit on employees
42(3) A **public body** shall limit the use of **personal information** in its custody or under its control to those of its **employees** 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 43.

FIPPA contains three key requirements that govern every use of **personal information** by a **public body** and its officers, staff, contractors and agents:

(i) Every use of **personal information** by or on behalf of the **public body** must be authorized under section 43 of FIPPA.

A **public body** can only use **personal information** for the purpose for which it was collected or compiled unless:

- the individual has consented to use for another purpose [clause 43(b)]; or
- use for another purpose is authorized under clause 43(a) or (c) of FIPPA.

(ii) Every use of **personal information** by or on behalf of the **public body** must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used, and

(iii) Access to and use of **personal information** by the **employees** – the officers, staff, contractors and agents – of the **public body** must be limited to those 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 43 of FIPPA.[180]

Example:

When preparing for a ministerial briefing note, a **department** must be careful to ensure that:

(i) **personal information** is only provided to those officials and staff of the department who need to know that information to prepare the briefing note; and

(ii) the **personal information** shared with officials and staff is limited to the minimum amount necessary to prepare the briefing note.

[180] There are similar limits respecting **personal health information** in section 20 of *The Personal Health Information Act* that apply to trustees, including **public bodies**. In addition, section 18 of that Act sets out specific controls that must be put in place respecting use of **personal health information**. *The Personal Health Information Ac*t, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

■ Authorized Uses of Personal Information - [Section 43]

> **Use of personal information**
> **43** A **public body** may use **personal information** only.....

Subsection 42(1) requires that every use of **personal information** in the custody or under the control of a **public body** by or on behalf of the public body must be authorized under section 43 of FIPPA.

Section 43 states that **personal information** may be used by or on behalf of the **public body** that has custody or control of the information only where one of the circumstances described in clause 43(a), (b) or (c) exists.

In practical terms, a **public body** must use **personal information** only

(i) for the purpose for which it was originally collected;

(ii) for a "consistent purpose" which meets the requirements in section 45 of FIPPA;

(iii) where the individual the **personal information** is about consents to its use for a different purpose; or

(iv) for a purpose for which the information may be disclosed to the **public body** under section 44, 47 or 48 of FIPPA.

As discussed above, "use" of **personal information** means using or dealing with the **personal information** within or for the purposes of the **public body** that has custody or control of the information.

Public bodies should undertake a review of their activities to ensure that **personal information** is being used by them, or on their behalf, in accordance with the requirements of FIPPA.

■ Use for the Original Purpose or for a Consistent Purpose - [Clause 43(a)]

Use of personal information
43 A **public body** may use **personal information** only

(a) for the purpose for which the information was collected or compiled under subsection 36(1) or for a use consistent with that purpose under section 45;

Consistent purposes
45 For the purpose of clauses 43(a) and 44(1)(a), a use or disclosure of **personal information** is consistent with the purpose for which the information was collected or compiled if the use or disclosure

(a) has a reasonable and direct connection to that purpose; and

(b) is necessary for performing the statutory duties of, or for delivering an authorized service or program or carrying out an activity of, the **public body** that uses or discloses the information.

Clause 43(a) contains two authorized uses of **personal information**:

(i) Use for the purpose for which the **personal information** was originally collected or compiled under subsection 36(1);

(ii) Use that is consistent with the purpose for which the **personal information** was collected or compiled.

1. Use for the purpose for which the personal information was originally collected or compiled

A **public body** may use **personal information** for the specific purpose for which it originally collected or compiled the information under section 36(1) of FIPPA.

This, of course, requires identification of the purposes for which the **personal information** was collected or compiled.

A "purpose" is an end, intention, aim, object, plan or project.[181] In clause 43(a), the "purpose" for which the **personal information** was collected or compiled is the end, aim or object to be achieved by collecting or compiling the **personal information** or what was intended to be accomplished by collecting or compiling the **personal information**.

The "purpose" for which **personal information** is collected or compiled must be authorized under subsection 36(1). Subsection 36(1) restricts collection of **personal information** to situations where:

(a) collection of the information is authorized by or under an **enactment** (a statute or regulation) of Manitoba or of Canada;

(b) the information relates directly to and is necessary for an existing service, program or activity of the **public body**; or

(c) the information is collected for **law enforcement** purposes or crime prevention.[182]

To "collect" **personal information** means to assemble or accumulate **personal information**;[183] to gather **personal information** together.[184]

To "compile" **personal information** means to collect and put together information, to make, compose or construct a collection of information by arrangement of materials collected from various sources.[185]

2. Use of personal information for a consistent purpose

Clause 43(a) also permits use of **personal information** by a **public body** where the proposed use is consistent with the purpose for which the information was originally collected or compiled.

Again, this requires identification of the purposes for which the **personal information** was originally collected or compiled.

---

181 *Black's Law Dictionary, 6th Edition*.

182 Subsection 36(1) is discussed earlier in this Chapter under *Collection of Personal Information*.

183 *The Concise Oxford Dictionary, 9th Edition*.

184 *Black's Law Dictionary, 6th Edition*. And see the discussion of the meaning of collection earlier in this Chapter, under *Collection of Personal Information*.

185 *The Compact Edition of the Oxford English Dictionary*.

"Consistent purpose" is defined in section 45 of FIPPA. To meet the test of consistent purpose, the proposed use must meet the requirements of both clauses 45(a) and (b):

(a) The proposed use must have a reasonable and direct connection to the purpose for which the **personal information** was originally collected or compiled [clause 45(a)].

A "reasonable" connection to the original purpose means a connection or link[186] that is justifiable or logical.[187]

A "direct" connection is one that is straightforward or unambiguous.[188]

A proposed use has a "reasonable and direct connection" to the original purpose for which the **personal information** was collected or compiled if there is a logical and clear link to the original purpose of collection, if the proposed new use logically flows from the original purpose.

(b) The proposed use must also be necessary:

- for performing the statutory duties of the **public body** that uses the **personal information**; or
- for delivering an authorized program or service or carrying out an activity of the **public body** that uses the **personal information** [clause 45(b)].

"Necessary" in this context means that the **public body** will be unable to properly or fully carry out its duties or activities, or deliver its service or program, without using the **personal information** in the proposed manner.

There are no hard and fast rules as to what constitutes a use for a "consistent purpose". One guideline to consider is whether a reasonable person would anticipate or expect the **personal information** to be used in the proposed way, even if this use was not spelled out at the time the **personal information** was collected. [189]

---

186 *The Concise Oxford Dictionary, 9th Edition*.

187 *The Concise Oxford Dictionary, 9th Edition*.

188 *The Concise Oxford Dictionary, 9th Edition*.

189 See, for example, B.C. Information and Privacy Commissioner Investigation Report 00-01:

Example:

The Policy and Planning Branch of a **department** uses **personal information** originally collected for the purpose of delivering a service to audit, monitor or evaluate the effectiveness of the service. This is use for a "consistent purpose" as:

- the use of **personal information** is directly related to the original purpose of the collection, as it is being used to audit, monitor or evaluate the service for which the information was originally collected; and

- it is necessary for the **public body** to audit, monitor or evaluate its service to ensure that it is properly carried out, and that problems and deficiencies are identified and addressed.

Example:

A **public body** wishes to expand an assistance program to include a set of people who were recently rejected under previous criteria because of age. Rather than collecting the same information again, the **public body** uses the information collected from these people in their original applications to determine eligibility under the new criteria. The use is consistent with the original purpose as the information was originally gathered to determine eligibility for a particular program and is being used for the same program because the eligibility criteria have recently changed.

http://www.llbc.leg.bc.ca/public/pubdocs/bcdocs/156693/2000/order00-01.htm.

■ Use with the Individual's Consent - [Clause 43(b)]

Use of personal information
43 A **public body** may use **personal information** only

(b) if the individual the information is about has consented to the use; or

Clause 43(b) permits a **public body** to use **personal information** for a purpose other than the original purpose for which the information was collected if the individual the information is about consents to this "different' use.

"Use" of **personal information** for a purpose other than the purpose for which it was originally collected is sometimes referred to as use for a 'secondary' purpose.

Under clause 87(h) of FIPPA the Lieutenant Governor in Council may make regulations under FIPPA respecting the giving of consents by individuals under FIPPA. At this time there are no regulations under FIPPA respecting consent.

The elements of a valid consent are discussed earlier in this Chapter, under *Consent and FIPPA*. An individual's consent to a different use of **personal information** for the purposes of clause 43(b) of FIPPA:

(i) must be clearly related to the proposed different use of the **personal information**;

(ii) must be knowledgeable (that is, informed);

(iii) must be voluntary; and

(iv) must not be obtained through misrepresentation.

Where possible, an individual's consent to a different use of his or her **personal information** should be in writing. If consent is given verbally, the **public body** should make a written record of the conversation and, where reasonable, send a letter to the individual confirming the consent.

An individual's consent to a different use of his or her **personal information** should include:

- a description of the particular **personal information** to be used;
- a clear and complete description of the different use to which the information is to be put (e.g. what new purpose the information will be used for; why it is necessary to use it for that new purpose; the consequences of refusing to consent to the new use of the information; etc.);
- a clear description of the **public body** to which the consent is being given, and of the program, service or activity of the **public body** that will be using the **personal information** for this different purpose;
- how long the consent will remain in effect (that is, when it expires);
- a statement that the consent can be withdrawn by notifying the **public body**, and a statement explaining the consequences of withdrawing the consent;
- the date of the consent (the date it is given);
- the name of the person giving the consent; and
- a signature, in the case of a written consent; etc.

Consent for a 'different' use must be obtained before the information is put to the 'different' use.

In limited circumstances, a consent for the purposes of clause 43(b) may be provided by certain persons authorized to act on behalf of the individual the information is about under section 79 of FIPPA.[190]

In the absence of consent, a **public body** cannot assume that it is authorized to use the **personal information** for a purpose that is different from the one for which the information was originally collected. Where there is no consent, authority to use the information for a different purpose must be found under clause 43(a) or 43(c) of FIPPA.

[190] Section 79 of FIPPA is discussed in Chapter 3, *Exercising Rights on Behalf of Another Person*.

A **public body** should not penalize individuals for refusing to consent to a 'different' use of **personal information** by denying them the benefit or service for which the **personal information** was originally collected. Individuals may find, however, that they are denied a benefit or service that would have been determined through the different use of the **personal information** if consent to the different use is requested and refused.

As a consent under clause 43(b) provides the **public body** with legal authority to use **personal information** for a purpose that is different from the purpose for which the **personal information** was originally collected, it is strongly recommended that legal counsel be consulted when drafting a consent document.

Also see Ombudsman's: *Use under FIPPA*.[191]

[191] This document can be found on the Ombudsman's website at: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

■ Use for a Purpose for which the Information May Be Disclosed to the Public Body - [Clause 43(c)]

Use of personal information
43 A **public body** may use **personal information** only

(c) for a purpose for which that information may be disclosed to the **public body** under section 44, 47 or 48.

Clause 43(c) permits a **public body** to use **personal information** for a purpose for which that information may be disclosed to the **public body** under section 44, 47 or 48 of FIPPA. These sections, which are discussed in detail later in this Chapter, permit disclosure of **personal information** for limited and specific purposes.

For example, as each **department** of the Government of Manitoba is a separate **public body** under FIPPA, sharing of **personal information** by one government **department** with another government **department** is a disclosure under FIPPA and must be authorized under section 44. Without clause 43(c), a **public body** would not be able to use **personal information** that could be disclosed to it.

Clause 43(c) recognizes that there are limited circumstances where it is appropriate for **a public body** to share **personal information** within the **public body** or for **public bodies** to share **personal information** with each other, particularly where the same **personal information** is required by another part of the **public body** or by more than one public body for legitimate programs and activities. In appropriate circumstances, clause 43(c) can reduce the number of times an individual must provide the same **personal information** to **public bodies** and can reduce the cost of gathering **personal information** required by more than one **public body**.

Note: The **public body** receiving the **personal information** must have authority to collect it under subsection 36(1) of FIPPA.

Also see Ombudsman Practice Note: *Use under FIPPA*.[192]

[192] This Practice Note can be found on the Ombudsman's website at: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

DISCLOSURE OF PERSONAL INFORMATION - [SECTIONS 42 AND 44] [193]

Sections 42 and 44 set out the rules for the disclosure of **personal information** in the custody or under the control of a **public body**.

Two of the Privacy Principles discussed earlier in this Chapter are particularly relevant to the disclosure of **personal information** by **public bodies**, and are reflected in sections 42 and 44 of FIPPA:

- Identifying Purposes; and
- Use, Retention and Disclosure Limitation.

■ Overview of Disclosure of Personal Information

Section 42 sets out the limits on the disclosure of **personal information** by **public bodies**.

(i) a **public body** can only disclose **personal information** if authorized to do so under section 44 of FIPPA; and

(ii) disclosure must be limited to the minimum amount of **personal information** necessary to accomplish the purpose for which it is disclosed.

This section of the Manual is broken down as follows:

- the meaning of 'disclosure';
- the relationship of authorized disclosure under section 44 to access to information under Part 2 of FIPPA;
- the limits on disclosure;

[193] Sections 20, 22, 23, 23.1, 23.2, 24, 24.1 and 25 of *The Personal Health Information Act* set out the rules respecting disclosure of **personal health information** by trustees, including **public bodies**. Section 27 of that Act prohibits the sale of **personal health information** except in the course of the sale of a practice or health care facility in strictly controlled circumstances.

- authorized disclosure – general requirements, including exercising discretion;

  and

- the authorized disclosures of **personal information** permitted by clauses 44(1)(a) to (dd).

Section 44 of FIPPA sets out the only circumstances in which a **public body** may disclose **personal information**.

Remember: **"personal information"** means "recorded information about an identifiable individual" and includes, but is not limited to, the information listed in clauses (a) to (n) of the definition of this term in subsection 1(1) of FIPPA.[194]

■ Meaning of Disclosure

"Disclosure" is not defined in FIPPA. A **public body** "discloses" **personal information** any time it makes the information known to, or reveals, exposes,[195] shows, provides, or sells **personal information** to, or shares the information with any person or entity outside the **public body** (who is not acting on behalf of the **pubic body**) by any means – for example, by providing copies, verbally, electronically or by any other means.

Sharing **personal information** with other **public bodies**, with the federal government or the government of another jurisdiction is disclosure of **personal information** that must be authorized under section 44 of FIPPA. Similarly, providing **personal information** to a non-government entity, a corporation or any other person outside the **public body** is disclosure of **personal information** that must be authorized under section 44.

It is important to note that, as each **department** of the Manitoba government is a separate **public body** under FIPPA, sharing of **personal information** between government **departments** is a "disclosure" under FIPPA.

---

194 The definition **"personal information"** is discussed in Chapter 2, under *Key Definitions*.

195 *The Concise Oxford Dictionary, 9th Edition*; *Black's Law Dictionary, 6th Edition*.

Example:

If Manitoba Family Services shares **personal information** with Manitoba Education and Advanced Learning, it is "disclosing" the information and the disclosure by Manitoba Family Services must be authorized under section 44 of FIPPA. For the purposes of FIPPA, Manitoba Family Services and Manitoba Education and Advanced Learning are two separate, distinct **public bodies**.

Remember: Manitoba Education and Advanced Learning will need authority to collect the **personal information** under subsection 36(1) of FIPPA, and will also need authority to collect the information indirectly (from a source other than the individual the information is about) under subsection 37(1) of FIPPA.

But, remember: when a **public body** shares **personal information** with a contractor or agent providing services to that **public body**, this is a "use" of **personal information**, as the agent or contractor is acting on behalf of the **public body**.[196]

■ Relationship of Authorized Disclosure under Section 44 to Access to Information under Part 2 of FIPPA

Part 2 – Access to Information – and Part 3 – Protection of Privacy – have distinct and separate purposes.[197]

Part 2 of FIPPA sets out a process for formally requesting and obtaining access to a **record** that is in the custody or under the control of a **public body**. The **record** may contain general information, **personal information** about the person making the request or **personal information** about another person. The right of access is subject to the specific and limited exceptions to disclosure set out in Part 2 of FIPPA, one of which (section 17) protects the privacy of individuals.

196 Discussed earlier in this Chapter, under *Use of Personal Information*.

197 See Chapter 1 for a discussion of the principles and purposes underlying the access to information provisions in Part 2 of FIPPA and the protection of privacy provisions in Part 3 of FIPPA.

Part 3 of FIPPA deals with information privacy and the protection of **personal information** – that is, recorded information about an identifiable individual. Part 3 sets out the obligations of a **public body** with respect to the collection, use, accuracy, retention, protection, disclosure and destruction of **personal information** in its custody or under its control.

Section 44 is found in Part 3 of FIPPA and sets out the situations in which a **public body** is authorized (is permitted) to disclose **personal information** in its day to day activities. A **public body** is authorized (permitted) to disclose **personal information** for the purposes set out in subsection 44(1), but is not required to do so (unless another law – for example, a court order or another statute – requires the disclosure).

Clause 44(1)(c) also specifically permits a **public body** to disclose **personal information** in response to an access request under Part 2 of FIPPA, subject to the exceptions to disclosure in Part 2.

Section 17 of FIPPA is one of the exceptions to disclosure in Part 2 of FIPPA. Section 17 balances the public's right of access to **records** in the custody or under the control of a **public body** and an individual's right of privacy with respect to his or her **personal information**. Section 17 protects privacy by providing a mandatory exception to the general right of access to **records** in Part 2 of FIPPA – section 17 requires a **public body** to refuse access to **personal information** where providing access would unreasonably invade the privacy of the individual the **personal information** is about.

If an applicant for access under Part 2 of FIPPA requests access to a **record** containing **personal information** about someone else, and providing access would unreasonably invade that other person's privacy, section 17 requires that the **head** of the **public body** refuse access to that **personal information**.

Also see Ombudsman Practice Note: *Distinguishing Between Access to Information Requests and Authorized Disclosures under FIPPA and PHIA.*[198]

[198] This Practice Note can be found on the Ombudsman's website at: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

■ Limits on Disclosing Personal Information - [Subsections 42(1) and (2)]

General duty of public bodies
42(1) A **public body** shall not use or disclose **personal information** except as authorized under this Division.

Limit on amount of information used or disclosed
42(2) Every use and disclosure by a **public body** of **personal information** must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed.

FIPPA contains two key requirements which govern every disclosure of **personal information** by or on behalf of a **public body**:

(i) Every disclosure of **personal information** by or on behalf of the **public body** must be authorized under subsection 44(1) of FIPPA.

(ii) Every disclosure of **personal information** by or on behalf of the **public body** must be limited to the minimum amount of information necessary to accomplish the purpose for which it is disclosed.[199]

When disclosing **personal information**, a **public body** must take precautions appropriate to the circumstances to ensure that the information is disclosed only to the intended recipient. These precautions include:

- taking reasonable steps to protect the **personal information** from unauthorized access or disclosure while it is being transmitted or sent to the intended recipient;

- verifying the identity of the recipient; etc.

[199] There are similar limits respecting disclosure of personal health information in section 20 of *The Personal Health Information Act* that apply to trustees of personal health information, including public bodies. In addition, section 18 of that Act sets out specific security safeguards that must be put in place respecting disclosures of personal health information. *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

Also see Ombudsman Practice Notes:

- *Disclosure under FIPPA;*
- *Privacy Considerations for Faxing Personal and Personal Health Information;*
- *Privacy Considerations for Emailing Personal and Personal Health Information.*[200]

[200] These Practice Notes can be found on the Ombudsman's website at: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

■ Authorized Disclosure of Personal Information - [Subsection 44(1)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only.....

1. Disclosure of personal information must be authorized

Subsection 42(1) requires that every disclosure of **personal information** in the custody or under the control of a **public body** must be authorized under section 44 of FIPPA.

Subsection 44(1) provides that **personal information** may be disclosed only if one of the circumstances described in clauses 44(1)(a) to (dd) applies.

2. Disclosure is authorized, or permitted, not required, under section 44

Under subsection 44(1), a **public body** "may" disclose **personal information** for one of the purposes listed in clauses (a) to (dd). The use of the word "may" in subsection 44(1) indicates that the **public body** can exercise its discretion when deciding whether or not to disclose the **personal information**. Subsection 44(1) authorizes or permits disclosure; it does not require disclosure.

In determining whether to disclose **personal information**:

(i) The **public body** must first determine whether or not there is authority to disclose the **personal information** under one or more of the clauses of subsection 44(1).

(ii) If there is authority in subsection 44(1) to disclose the **personal information**, the **public body** must then determine whether or not to exercise its discretion to disclose.

In exercising this discretion, the **public body** must consider whether it is appropriate to disclose the information in the circumstances, taking into account both the potential harm that would result from disclosure (including the harm to an individual's privacy) and the consequences of not disclosing the information.

The following is a summary of some of the general principles that apply to the exercise of a discretion:

> .. the discretion must be exercised by the authority to which it is committed, which must act on its own and not under the dictation of any other body, and ... it must be willing to exercise its discretion in each individual case which comes before it. The authority must act in good faith, must have regard to all relevant considerations and must not be swayed by irrelevant considerations, must not seek to promote purposes alien to the letter or to the spirit of the legislation which gives it power to act, and must not act arbitrarily or capriciously.[201]

(iii) If the decision is to disclose **personal information**, the **public body** must decide how much **personal information** should be disclosed.

The **public body** must keep in mind the requirement of subsection 42(2) of FIPPA that every disclosure must be "limited to the amount of information necessary to accomplish the purpose for which it is disclosed".

Some clauses of subsection 44(1) are in reality not discretionary. For example, a **public body** really has no discretion to refuse to disclose **personal information** when:

- disclosure is required (as opposed to authorized) by another Act or regulation of Manitoba or Canada [clause 44(1)(e)], or

- disclosure is required in response to a properly authorized, drafted and served subpoena, warrant or other order of a court or tribunal [clause 44(1)(m)].

---

[201] *Administrative Law* by Evans, Janisch, Mullan and Risk (1980), at page 623.

3. Disclosure is authorized only in the circumstances set out in subsection 44(1)

Clauses 44(1)(a) to (dd) of FIPPA list the only circumstances in which a **public body** may disclose **personal information**. The **public body** cannot disclose **personal information** in circumstances that are not included in subsection 44(1) of FIPPA.

Public bodies should undertake a review of their activities, information sharing agreements, etc. to ensure that **personal information** is being disclosed in accordance with the requirements of FIPPA.

■ Disclosure for the Original or a Consistent Purpose - [Clause 44(1)(a)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(a) for the purpose for which the information was collected or compiled under subsection 36(1) or for a use consistent with that purpose under section 45;

Consistent purposes
45 For the purpose of clauses 43(a) and 44(1)(a), a use or disclosure of **personal information** is consistent with the purpose for which the information was collected or compiled if the use or disclosure

(a) has a reasonable and direct connection to that purpose; and

(b) is necessary for performing the statutory duties of, or for delivering an authorized service or program or carrying out an activity of, the **public body** that uses or discloses the information.

Clause 44(1)(a) contains two authorized disclosures of **personal information**:

(i) disclosure for the purpose for which the information was originally collected or compiled under subsection 36(1);

(ii) disclosure for a use that is consistent with the purpose for which the information was collected or compiled.

1. Disclosure for the purpose for which the personal information was originally collected or compiled under subsection 36(1)

A **public body** may disclose **personal information** if is it necessary to do so to accomplish the purpose for which the information was originally collected or compiled by or for the **public body**. This, of course, requires identification of the purposes for which the **personal information** was originally collected or compiled.

A "purpose" is an end, intention, aim, object, plan or project.[202] In clause 44(1)(a), the "purpose" for which the **personal information** was collected or compiled is the end, aim or object to be achieved by collecting or compiling the **personal information** or what was intended to be accomplished by collecting or compiling the **personal information**.

The "purpose" for which a **public body** collects or compiles **personal information** must be authorized under subsection 36(1) of FIPPA. Subsection 36(1) restricts collection of **personal information** to situations where:

(a) collection of the information is authorized by or under an **enactment** (a statute or regulation) of Manitoba or of Canada; or

(b) the information relates directly to and is necessary for an existing program or activity of the **public body**; or

(c) the information is collected for **law enforcement** purposes or crime prevention.[203]

To "collect" **personal information** means to assemble or accumulate **personal information**;[204] to gather **personal information** together.[205]

To "compile" **personal information** means to collect and put together information, to make, compose or construct a collection of information by arrangement of materials collected from various sources.[206]

---

202 *Black's Law Dictionary, 6th Edition*.

203 Subsection 36(1) is discussed earlier in this Chapter under *Collection of Personal Information.*

204 *The Concise Oxford Dictionary, 9th Edition*.

205 *Black's Law Dictionary, 6th Edition*.

206 *The Compact Edition of the Oxford English Dictionary*.

2. Disclosure of personal information for a consistent purpose

Clause 44(1)(a) also permits disclosure of **personal information** by a **public body** where the disclosure is consistent with the purpose for which the information was originally collected or compiled. Again, this requires that the purposes of collection be identified.

"Consistent purpose" is defined in section 45 of FIPPA. To meet the test of consistent purpose, the disclosure must meet the requirements of both clauses 45(a) and (b):

(a) The disclosure must have a reasonable and direct connection to the purpose for which the **personal information** was originally collected or compiled [clause 45(a)].

A "reasonable" connection to the original purpose means a connection or link[207] that is justifiable or logical.[208]

A "direct" connection is one that is straightforward or unambiguous.[209]

A disclosure has a "reasonable and direct connection" to the original purpose for which **personal information** was collected if there is a logical and clear link to the original purpose, if the disclosure logically flows from the original purpose.

(b) The disclosure must be necessary:

- for performing the statutory duties of the **public body** that discloses the **personal information**, or
- for delivering an authorized service or program or for carrying out an activity of the **public body** that discloses the **personal information** [clause 45(b)].

[207] *The Concise Oxford Dictionary, 9th Edition*.

[208] *The Concise Oxford Dictionary, 9th Edition*.

[209] *The Concise Oxford Dictionary, 9th Edition*.

"Necessary" in this context means that the **public body** will be unable to properly or fully carry out its duties or activities, or deliver its service or program, without disclosing the **personal information** in the proposed manner.

There are no hard and fast rules as to what constitutes a disclosure for a "consistent purpose". One guideline to consider is whether a reasonable person would anticipate or expect the **personal information** to be disclosed in the proposed way, even if this disclosure was not spelled out at the time the **personal information** was collected.

■ Disclosure with the Individual's Consent - [Clause 44(1)(b)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(b) if the individual the information is about has consented to its disclosure;

Clause 44(1)(b) permits a **public body** to disclose **personal information** outside the **public body** if the individual the information is about consents to the disclosure.

Under clause 87(h) of FIPPA, the Lieutenant Governor in Council may make regulations under FIPPA respecting the giving of consents by individuals under FIPPA. At this time, there are no regulations respecting consent under FIPPA.

The elements of a valid consent are discussed earlier in this Chapter, under *Consent and FIPPA*. An individual's consent to disclosure of his or her **personal information** for the purposes of clause 44(1)(b) of FIPPA:

(i) must be clearly related to the proposed disclosure of the **personal information**;

(ii) must be knowledgeable (that is, informed);

(iii) must be voluntary; and

(iv) must not be obtained through misrepresentation.

Where possible, an individual's consent to disclosure of his or her **personal information** should be in writing. If consent is given verbally, the **public body** should make a written record of the conversation and, where reasonable, send a letter to the individual confirming the consent.

The individual's consent should include:

- a description of the particular **personal information** to be disclosed;
- a clear descript
- ion of the **public body** proposing to disclose the **personal information** (the **public body** to whom the consent to disclose is being given);
- a description of the recipient of the information – the **public body**, person or organization to whom the **personal information** is to be disclosed – and the purpose of the disclosure;
- a clear and complete description of the purpose of the disclosure; (e.g. why it is necessary to disclose the information; the purpose for which it is being disclosed and for which it will be used by the recipient; the consequences of refusing the consent; etc.);
- how long the consent will remain in effect (that is, when it expires);
    - a statement that the consent can be withdrawn by notifying the **public body**, and a statement explaining the consequences of withdrawing the consent;
- the date of the consent (the date it is given);
- the name of the person giving the consent; and
- a signature, in the case of a written consent; etc.

Consent to disclosure may be sought at the time the **personal information** is collected if the disclosure is anticipated. If the disclosure is not anticipated at the time the information is collected, consent may be obtained at a subsequent time, but must be obtained before the proposed disclosure takes place.

In limited circumstances, a consent to disclosure of **personal information** for the purposes of clause 44(1)(b) may be provided by certain persons authorized to act on behalf of the individual the information is about under section 79 of FIPPA.[210]

[210] Section 79 is discussed in Chapter 3, under *Exercising Rights on Behalf of Another Person*.

In the absence of consent to disclosure, a **public body** cannot assume that it is authorized to disclose the **personal information**. Where there is no consent, authority to disclose **personal information** must be found in another clause of subsection 44(1) of FIPPA.

A **public body** should not penalize individuals for refusing to consent to a disclosure of their **personal information** that is not otherwise permitted by subsection 44(1) by denying them the benefit or service for which the **personal information** was originally collected. Individuals may find, however, that they are denied another benefit or service that would have been determined through the proposed disclosure of the **personal information** where they have refused to consent to the disclosure.

Also see the Ombudsman's *Disclosure under FIPPA*.[211]

[211] This document can be found on the Ombudsman's website at: http://www.ombudsman.mb.ca/documents_and_files/practice-notes.html.

■ Disclosure in Accordance with Part 2: Access to Information - [Clause 44(1)(c)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (c) in accordance with Part 2;

Clause 44(1)(c) allows a **public body** to disclose **personal information** in response to a request for access made under Part 2 of FIPPA. But, such a disclosure is subject to the exceptions to disclosure in sections 17 to 32 of Part 2 of FIPPA.

Section 17 of Part 2 balances the public's right of access to **records** in the custody or under the control of a **public body** and an individual's right of privacy with respect to his or her **personal information**. Section 17 protects privacy by providing a mandatory exception to the right of access under Part 2 for **personal information** about a **third party**. Under section 17, the **head** of a **public body** is required to refuse to disclose to an **applicant** requesting access under Part 2 **personal information** about another individual if the disclosure would be an "unreasonable invasion" of that other individual's privacy.

Other exceptions to disclosure in Part 2 that may protect privacy include:

Section 18	Business Interests of **third parties**
Section 24	Individual or public safety
Clause 25(1)(e)	Life or safety of **law enforcement** officer or others
Clause 25(1)(f)	Right to a fair trial or impartial adjudication
Clause 25(1)(l)	Confidential information in a correctional **record**
Clause 25(1)(m)	Author of, or person quoted in, a **law enforcement** record
Subsection 27(2)	Solicitor-client privilege of another person
Section 30	Confidential evaluations about the **applicant**.[212]

Note: Subsection 44(1) and Part 2 of FIPPA do not prevent a policy, custom or practice of routine disclosure of **personal information** by a **public body** to the individual the information is about.[213] The **public body** will, of course, want to have measures in place to verify identity before providing **personal information**, etc.

[212] Section 17 and the other exceptions to disclosure in Part 2 of FIPPA are discussed in Chapter 4.

[213] Clause 3(a) is discussed in Chapter 2, under *Procedures not Affected by FIPPA*.

■ Disclosure to Comply with an Enactment or Agreement under an Enactment - [Clause 44(1)(d)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (d) for the purpose of complying with an **enactment** of Manitoba or Canada, or with a treaty, arrangement or agreement entered into under an **enactment** of Manitoba or Canada;

Clause 44(1)(d) states that **personal information** may be disclosed by a **public body** in either of two situations:

(i) if the disclosure is for the purpose of complying with an **enactment** of Manitoba or Canada, or

(ii) if the disclosure is for the purpose of complying with a treaty, arrangement or agreement entered into under an **enactment** of Manitoba or Canada.

1. Disclosure to comply with an enactment of Manitoba or Canada

An **"enactment"** is defined in subsection 1(1) of FIPPA as "an Act or regulation". For the purposes of clause 44(1)(d),

- an "Act" is a statute passed by the Legislative Assembly of Manitoba or by the Parliament of Canada.
- a "regulation" is a law made under the authority of a statute by the Lieutenant Governor in Council (in the case of Manitoba), the Governor General in Council (in the case of Canada), a minister, etc.

To "comply" with an **enactment** means to act in accordance with[214] or fulfill the requirements of the statute or regulation. Disclosure "for the purpose of complying with" an **enactment** of Manitoba or Canada means that **personal information** may be disclosed to enable the **public body** to fulfill the requirements of or deliver a service or program or carry out an activity that is authorized by a statute or regulation of Manitoba or Canada. Without the disclosure, the aims or objectives of the statute or regulation could not be met.

The relevant statute or regulation may not specifically refer to disclosure of **personal information**.

Clause 44(1)(d) does not authorize a **public body** to disclose **personal information** under the authority of a statute or regulation of another province or territory, or of a foreign country.

2. Disclosure to comply with a treaty, arrangement or agreement entered into under an enactment of Manitoba or Canada.

A "treaty" is a compact made between two or more independent nations with a view to the public welfare,[215] a binding agreement between states.[216] An "arrangement" is a settlement of mutual relations or claims between parties.[217]

An "agreement" is a mutual understanding, an arrangement between parties as to a course of action,[218] a contract.[219] An agreement is more precise than an arrangement and is usually, although not always, in writing.

For disclosure of **personal information** to be authorized under this aspect of clause 44(1)(d), the treaty, arrangement or agreement under which **personal information** is to be disclosed or exchanged must be entered into under the authority of a statute or regulation of Manitoba or of Canada.

---

214 *The Concise Oxford Dictionary, 9th Edition*.

215 *Black's Law Dictionary, 6th Edition*.

216 *The Dictionary of Canadian Law*.

217 *The Compact Edition of the Oxford English Dictionary*.

218 *The Concise Oxford Dictionary, 9th Edition*.

219 *The Dictionary of Canadian Law*.

Example:

Under subsection 22.1(1.1) of *The Retail Sales Tax Act*, the Minister of Finance may enter into an agreement with the Government of Canada for the collection of taxes. Disclosure of **personal information** by the Minister to the Government of Canada to comply with this agreement would be authorized under clause 44(1)(d) of FIPPA.

■ Disclosure Authorized or Required by an Enactment - [Clause 44(1)(e)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (e) in accordance with an **enactment** of Manitoba or Canada that authorizes or requires the disclosure;

Clause 44(1)(e) states that a **public body** may disclose **personal information** where an **enactment** of Manitoba or Canada authorizes or requires the disclosure. It specifically recognizes that another statute or regulation may provide for the disclosure of **personal information**. That is, if another statute or regulation authorizes or requires a **public body** to disclose **personal information**, the disclosure is authorized under FIPPA.

Clause 44(1)(e) complements the authority to disclose **personal information** under clause 44(1)(d). While clause 44(1)(d) authorizes disclosure of **personal information** to comply with Manitoba or federal statutes or regulations whose aims or objectives could not reasonably be met without disclosure taking place, clause 44(1)(e) covers those Manitoba or federal statutes or regulations that specifically deal with disclosure.

1. Meaning of "enactment"

An **"enactment"** is defined in subsection 1(1) of FIPPA as "an Act or regulation". For the purposes of clause 44(1)(e) of FIPPA,

- an "Act" of Manitoba or Canada is a statute passed by the Legislative Assembly of Manitoba or by the Parliament of Canada.
- a "regulation" is a law made under the authority of a statute by the Lieutenant Governor in Council (in the case of Manitoba), by the Governor General in Council (in the case of Canada), by a minister of the government of Manitoba or Canada, etc.

2. Disclosure authorized by an enactment

Disclosure of **personal information** is "authorized" by an **enactment** where the disclosure is permitted but not required.

Words such as "may disclose", "may provide", "has a discretion to disclose" indicate authority to disclose.

Example:

Clause 55(2.2) of *The Family Maintenance Act* states that a 'designated officer' may provide information collected to enforce orders for spousal and child support in Manitoba to "an appropriate authority in a reciprocating jurisdiction for the purpose of enforcement of a support order as defined in *The Inter-jurisdictional Support Orders Act."*

3. Disclosure required by an enactment

Disclosure is "required" by an **enactment** where there is an obligation to disclose.

Words such as "shall" disclose or "must" disclose, provide, etc. indicate that disclosure is required.

Where disclosure of **personal information** is required (as opposed to authorized) by another Act or regulation of Manitoba or Canada, the **public body** does not have any real discretion to refuse to disclose the **personal information**.

Examples of Manitoba statutes that require disclosure of **personal information** by employees of **public bodies**:

- Section 18 of *The Child and Family Services Act*. Under this provision, any person who has information that leads him or her reasonably to believe that a child is or might be in need of protection "shall report the information" to a child and family services agency or to a regional office of the Department of Family Services, even if the information is obtained in the course of professional duties or a confidential relationship. This requirement to disclose information extends, for example, to teachers employed by **educational bodies**, public health nurses employed by **health care bodies**, public health professionals employed by the government, etc.

- Subsections 55(2) and (2.3) of *The Family Maintenance Act* provide that a person, government or agency served with a request from a 'designated officer' for information respecting the whereabouts, financial means, assets and liabilities of a person required to make payments under a maintenance order, etc. "shall provide" the requested information without fee within 21 days of the request.

■ Disclosure to a Minister or Elected Official - [Clause 44(1)(f)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(f) to a **minister** or an elected official of the **public body**, if the information is necessary to carry out his or her responsibilities;

"Minister" means a member of Cabinet (that is, a member of the Executive Council of the Government of Manitoba appointed under *The Executive Government Organization Act*).[220] The reference to "a **minister**" in clause 44(1)(f) includes any **minister** of the government, and also includes:

(a) another minister acting for the minister;

(b) if the office is vacant, another minister who is designated to act in the office by Order in Council;

(c) the minister's successors in office, and

(d) the minister's deputy minister.[221]

"Elected official of the **public body**" means a person elected to an office of the **public body** that has custody or control of the **personal information**. Examples include:

- a municipal councillor,
- a trustee of a public school board.

Clause 44(1)(f) does not authorize disclosure of **personal information** to an elected official of another **public body** (unless he or she is a **minister** of the Government of Manitoba).

---

[220] See the definitions **"minister"** and **"Cabinet"** in subsection 1(1) of FIPPA.

[221] Subsection 31(1) of *The Interpretation Act* of Manitoba, C.C.S.M. c.I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

Under clause 44(1)(f), **personal information** may be disclosed only if the information is necessary for the **minister** or the elected official to carry out his or her responsibilities. "Necessary" in this context means that the **minister** or official will be unable to properly or fully carry out his or her responsibilities without the **personal information**. That is, the **minister** or elected official must 'need to know' the **personal information** to carry out his or her responsibilities as a **minister** or as an elected official of the **public body**.

Example:

A **department** preparing a briefing note for the **minister** must be careful to:

(i) limit any **personal information** included in the briefing note to the information that the minister needs to know to carry out his or her responsibilities; and

(ii) limit the **personal information** in the briefing note to the minimum amount necessary for the **minister** to carry out his or her responsibilities.

■ Disclosure for a Common or Integrated Service, Program or Activity - [Clause 44(1)(f.1)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (f.1) to an officer or **employee** of a **public body**, for the purpose of delivering a common or integrated service, program or activity, if the information is necessary to deliver the service, program or activity and the officer or **employee** to whom the information is disclosed needs the information to carry out his or her responsibilities;[222]

This provision permits disclosure of **personal information** between officers and **employees** of **public bodies** that are working together to deliver a common or integrated program, service or activity, subject to strict limits and conditions.

Clause 44(1)(f.1) contains 4 requirements, all of which must be met for disclosure of **personal information** to be authorized:

(i) disclosure must be to an officer or **employee** of a **public body**;

(ii) the disclosure must be for the purpose of delivering a common or integrated service, program or activity;

(iii) the **personal information** to be disclosed must be necessary to deliver the service, program or activity; and

(iv) the officer or **employee** to whom the **personal information** is disclosed needs the information to carry out his or her responsibilities.

[222] Added to FIPPA by *The Freedom of Information and Protection of Privacy Amendment Act*, S.M. 2008 c. 40. The amending Act can be found at: http://web2.gov.mb.ca/laws/statutes/2008/c04008e.php.

1. Disclosure to officer or employee of a public body

Clause 44(1)(f.1) permits disclosure of **personal information** to an officer or **employee** of a **public body** that falls under FIPPA .

It does not permit disclosure to an organization that is not a **public body** that falls under FIPPA – for example, for the purposes of a program offered in partnership with a private sector organization.[223]

"**Employee"** is defined in subsection 1(1) of FIPPA to include "a person who performs services for the **public body** under a contract or agency relationship with the **public body**".

Remember: under FIPPA, each Manitoba government **department** is a separate **public body**.

2. "Common or integrated service, program or activity"

Clause 44(1)(f.1) permits disclosure to another **public body** for the purpose of delivering a common or integrated service, program or activity.

The phrase "common or integrated service, program or activity" is not defined in FIPPA. Generally, it is understood to mean:

- a single service, program or activity that is delivered by two or more **public bodies** (a common “service, program or activity"); or

- a service, program or activity that has several distinct components, each of which may be delivered by a separate **public body**, but which together constitute the service, program or activity. That is, each component is necessary for the service, program or activity (an “integrated service program or activity”).

Clause 44(1)(f.1) only permits disclosure of **personal information** to the officer or **employee** of a **public body** whose participation is integral – that is, necessary – to the common or integrated service, program or activity, in the sense that the service, program or activity would not function without its participation.

[223] Which bodies are public bodies that fall under FIPPA is discussed in Chapter 2, under *Public Bodies that Fall Under FIPPA*.

For example, a nursing practicum program requires the participation of both the **educational body** and the **health care body**; the program could not function without the services of each **public body**. In contrast, a situation where several **public bodies** have contracts with the same service provider is not a common or integrated service, program or activity.[224]

Clause 44(1)(f.1) permits sharing of **personal information** between the **public bodies** participating in order to deliver a service, program or activity to a client, etc. Simply having a common client does not mean that the service, program or activity is a "common or integrated" one.

Legislative authority setting out the criteria for a common or integrated program is a clear indication that a service, program or activity is a "common or integrated" one. In the absence of legislation, factors that help determine whether a service, program or activity is a "common or integrated" one include:

- a 'documented structure' – such as a formal agreement or arrangement for working together;
- evidence of joint planning by the **public bodies**;
- common goals expressed by the **public bodies**;
- evidence of collaboration or cooperation in delivery.

3. The information to be disclosed must be necessary to deliver the common or integrated service, program or activity.

Personal information is necessary to deliver a service, program or activity if it is required for or essential in order to deliver it.[225]

The **public bodies** participating must determine the specific elements of **personal information** that are needed to properly deliver the common or integrated service, program or activity, and must limit disclosure to the **personal information** that is necessary for this purpose.

---

[224] Based on Alberta *Freedom of Information and Protection of Privacy Act, Guidelines and Practices*, found at: http://www.servicealberta.ca/foip/resources/guidelines-and-practices.cfm.

[225] *The Concise Oxford Dictionary, 9th Edition*.

This specific requirement reinforces the requirement in subsection 42(2) of FIPPA to limit all disclosures of **personal information** to the minimum amount necessary to accomplish the intended purpose.

4. The public body officer or employee to whom the information is disclosed must "need the information to carry out his or her responsibilities".

That is, the **public body** disclosing the **personal information** must satisfy itself that the **public body** officer or **employee** to whom the information will be disclosed "needs to know" the information to properly deliver the common or integrated service, program or activity.

In keeping with the "Openness" Privacy Principle, **public bodies** delivering a common or integrated service, program or activity should consider notifying individuals participating in it of the nature of the service, program or activity, of the **public bodies** involved and of the sharing of **personal information**.

■ Disclosure to Manage or Administer Personnel - [Clause 44(1)(g)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (g) for the purpose of managing or administering personnel of the Government of Manitoba or the **public body**;

Clause 44(1)(g) permits a **public body** to disclose **personal information** for the purpose of:

- managing or administering its own personnel; or
- managing or administering the personnel of the Government of Manitoba generally.

To "manage" means to organize, regulate, be in charge of.[226]

To "administer" means to attend to the running of (business affairs, etc.); manage; be responsible for the implementation of.[227]

"Personnel" means a body of employees.[228]

The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[229] and is a broader concept than **"department"** or **"public body"**.

"Managing or administering personnel" in the context of clause 44(1)(g) includes all aspects of the internal management and administration of the human resources of a specific **public body** and also includes the government-wide management and administration of government personnel through the Manitoba Civil Service Commission.

---

226 *The Concise Oxford Dictionary, 9th Edition*.

227 *The Concise Oxford Dictionary, 9th Edition.*

228 *The Concise Oxford Dictionary, 9th Edition*.

229 *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act,* C.C.S.M. c.I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

Management of personnel refers to aspects of the management of personnel of a **public body** or the Government of Manitoba that relate to the duties and responsibilities of employees.[230] It includes things such as:

- staffing requirements;
- job classification, recruitment and selection;
- salary and benefits;
- hours and conditions of work;
- leave management;
- performance review;
- training;
- termination of employment and lay**–**off;
- management of personal service contracts of contract employees, etc.

Administration of personnel consists of all aspects of a **public body's** internal management, other than personnel management, that are necessary to support the delivery of programs and services. Administration includes business planning, and financial, contracts, property, information and risk management. [231]

"Managing or administering personnel" does not include management of independent contractors and consultants.

Disclosure of **personal information** for the purposes of managing or administering personnel of the Government of Manitoba can include disclosure to other **public bodies** or, in the case of government **departments**, to other **departments** or to the Manitoba Civil Service Commission.

However, all disclosures must be necessary for the purpose of carrying out official duties relating to the management or administration of personnel of the **public body** disclosing the **personal information** or of personnel of the Government of Manitoba.
Clause 44(1)(g) does not permit disclosure of personnel related information for purposes unrelated to official duties relating to the management or administration of personnel of the **public body** or of the government.

---

[230] See Alberta Information and Privacy Commissioner Investigation Report 2001-IR-006, found at: http://www.oipc.ab.ca/ims/client/upload/2001-IR-006.pdf.

[231] See Alberta Information and Privacy Commissioner Investigation Report 2001-IR-006, found at: http://www.oipc.ab.ca/ims/client/upload/2001-IR-006.pdf.

Also, as is the case with all **personal information** in the custody or under the control of a **public body**, the **public body** must limit the amount of **personal information** disclosed to the "minimum amount necessary" to manage or administer its personnel.[232]

Keeping in mind the "Openness" Privacy Principle, a **public body** may want to consider informing its **employees**, in a general way, of:

- what **personal information** about them is disclosed within the personnel management system of the **public body**, to whom and for what purposes; and

- how employees may obtain access to, and request corrections of, their **personal information**.

Some **public bodies** may be required to provide this and other information to **employees** under a collective agreement or other contract of employment.

[232] Subsection 42(2) of FIPPA, discussed earlier in this Chapter, under *Disclosure of Personal Information – Limits on Disclosing Personal Information*.

■ Disclosure to the Manitoba Auditor General, etc. for Audit Purposes - [Clause 44(1)(h)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (h) to the Auditor General or any other person or body for audit purposes;

Clause 44(1)(h) permits disclosure of **personal information** to the Auditor General or to other persons or bodies for the purposes of an audit.

An "audit" is an official examination of accounts or a systematic review[233] of the activities of the Government of Manitoba or a **public body**.

The Auditor General is an independent **officer of the Legislative Assembly** who is appointed and operates under the authority of *The Auditor General Act*. The Auditor General is responsible for examining the accounts and records of the Government of Manitoba and for reporting his or her findings to the Legislative Assembly.

Clause 44(1)(h) permits disclosure of **personal information** to the Manitoba Auditor General and to other persons or bodies for the purposes of an audit. "Person" means a natural person (a human being) and also includes a corporation and the heirs, executors, administrators or other legal representatives of a person.[234]

Disclosure under clause 44(1)(h) can include disclosure to:

- The Auditor General of Manitoba;
- an internal audit unit;

---

233 *The Concise Oxford Dictionary, 9th Edition.*

234 *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act* , C.C.S.M. c.I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

- a centralized audit unit such as Internal Audit of the Department of Finance; and

- persons or bodies retained under contract by the **public body** to carry out an audit.

As is the case with all disclosures under FIPPA, disclosure under clause 44(1)(h) is limited to the minimum amount of **personal information** necessary to accomplish the audit [subsection 42(2) of FIPPA].

If the audit is done by a person or body retained under a contract, the contract should include provisions respecting the use, protection and disclosure of **personal information** provided that are consistent with the requirements of FIPPA.

■ Disclosure to the Government of Canada to Monitor, Evaluate or Audit Cost Shared Programs or Services - [Clause 44(1)(i)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (i) to the Government of Canada in order to facilitate the monitoring, evaluation or auditing of shared cost programs or services;

To "monitor" a shared cost program or activity means to check or maintain regular surveillance[235] over the program or service.

To "evaluate" a shared cost program or activity means to assess or appraise it.[236]

An "audit" is an official examination of accounts or a systematic review[237] of the activities respecting the shared cost program or service.

The "Government of Canada" includes the various departments and agencies of the Government of Canada.

Examples of shared cost programs or services include:

- the labour market development program transferred by the Government of Canada to Manitoba in 1997;
- the immigrant realignment services transferred by the Government of Canada to Manitoba in 1998.

There may occasionally be overlap between this clause, clause 44(1)(a), (disclosure for a consistent purpose) clause 44(1)(h) (disclosure for audit purposes) and clause 44(1)(j.1) (disclosure for evaluation or monitoring or research and planning).

---

235 *The Concise Oxford Dictionary, 9th Edition*.

236 *The Concise Oxford Dictionary, 9th Edition*.

237 *The Concise Oxford Dictionary, 9th Edition.*

■ Disclosure to Determine or Verify Suitability or Eligibility - [Clause 44(1)(j)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (j) for the purpose of determining or verifying an individual's suitability or eligibility for a program, service or benefit;

Clause 44(1)(j) permits a **public body** to disclose **personal information** for either of two purposes:

(i) to determine suitability or eligibility for a program, service or benefit; or

(ii) to verify suitability or eligibility for a program, service or benefit.

1. Disclosure to determine suitability or eligibility for a program, service or benefit

Many programs, services or benefits provided by the Government of Manitoba or by **public bodies** have criteria that must be met for an individual to qualify to participate in the program or receive the service or benefit.

Clause 44(1)(j) permits a **public body** to disclose **personal information** to another **public body,** or to another organization or agency, where disclosure of the information is necessary to determine whether or not an individual meets the suitability or eligibility criteria of a particular program, service or benefit.

"Suitable" means that the individual is fit and appropriate[238] to participate in a program or receive a service or benefit.

[238] *Black's Law Dictionary, 6th Edition*.

"Eligible" means that the individual is qualified, fit or entitled[239] to participate in a program or receive a service or benefit.

Normally, the need to determine suitability or eligibility will arise when an application is made by the individual the **personal information** is about, or by a person authorized to act on his or her behalf, to participate in a program or receive a service or benefit.

2. Disclosure to <u>verify</u> suitability or eligibility for a program, service or benefit

Clause 44(1)(j) also permits a **public body** to disclose **personal information** to another **public body,** and to other organizations and agencies, if disclosure of the information is necessary to verify whether or not an individual met or continues to meet the suitability or eligibility criteria of a particular program, service or benefit.

To "verify" suitability or eligibility means to confirm, substantiate, authenticate, check or test[240] the appropriateness, fitness, qualifications or entitlement of an individual to participate in or receive, or continue to participate in or receive, a program, service or benefit.

Normally, verification occurs when an individual is already participating in the program or receiving the benefit or service, and the **public body**, organization or agency operating or delivering the program, service or benefit is checking to confirm that the individual was originally fit or qualified, or continues to be fit or qualified, to do so.

Verification of suitability or eligibility may be done on a regular basis, on a random basis or as a result of information received.

An individual will not always be informed that verification of his or her suitability or eligibility to participate in a program or receive a service or benefit is taking place.

---

239 *Black's Law Dictionary, 6th Edition; The Concise Oxford Dictionary, 9th Edition*.

240 *Black's Law Dictionary, 6th Edition*.

■ Disclosure for Evaluation or Monitoring or for Research and Planning - [Clause 44(1)(j.1)][241]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (j.1) for the purpose of
>
> (i) evaluating or monitoring a service, program or activity of the Government of Manitoba or the **public body**; or
>
> (ii) research and planning that relates to a service, program or activity of the Government of Manitoba or the **public body**;

1. Evaluating or monitoring a service, program or activity [Paragraph 44(1)(j.1)(i)]

Paragraph 44(1)(j.1)(i) permits a **public body** to disclose **personal information** for the purpose of:

- evaluating or monitoring a service, program or activity of the Government of Manitoba in the broad, 'corporate' sense;

  The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[242] and is a broader concept than **"department"** or **"public body"**.

---

[241] Clause 44(1)(j.1) was added to FIPPA by *The Freedom of Information and Protection of Privacy Amendment Act*, S.M. 2008 c. 40. The amending Act can be found at: http://web2.gov.mb.ca/laws/statutes/2008/c04008e.php.

[242] *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act*, C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

- evaluating or monitoring a service, program or activity of the **public body** that is disclosing the **personal information**.

In this context, to "evaluate" means to assess or appraise[243] a service, program or activity of the Government of Manitoba or of the **public body** disclosing the **personal information**. For example, a program could be 'evaluated' to assess whether it is effective.

To "monitor" means to check or maintain regular surveillance[244] over the service, program or activity of the Government of Manitoba or of the **public body** disclosing the **personal information**. For example, a **public body** might regularly monitor the way in which a service is being provided to ensure that it is being done properly.

2. Research and planning that relates to a service, program or activity [paragraph 44(1)(j.1)(ii)]

Paragraph 44(1)(j.1)(ii) permits a **public body** to disclose **personal information** for the purpose of:

- research and planning that relates to a service, program or activity of the Government of Manitoba in the broad, 'corporate' sense.

  The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[245] and is a broader concept than **"department"** or **"public body"**.

- research and planning that relates to a service, program or activity of the **public body** that is disclosing the **personal information**.

Note that "research" and "planning" are linked in this provision.

In this context, "research" means to investigate or closely study something,[246] usually in a systematic way in order to establish facts and reach new conclusions.

---

243 *The Concise Oxford Dictionary, 9th Edition*.

244 *The Concise Oxford Dictionary, 9th Edition*.

245 *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act*, C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

246 *The Compact Edition of the Oxford English Dictionary*.

To "plan" means to devise or design a formulated or organized method according to which something is to be done; to develop a scheme of action, project or design.[247]

Research and planning that relates to a program could involve:

- a systematic, detailed study of the program to determine how it is operating; whether it is achieving the intended purposes, and why (or why not); what problems have arisen; etc.; and

- the subsequent development of a plan to improve the effectiveness of the program or to expand it.

[247] *The Compact Edition of the Oxford English Dictionary*.

■ Disclosure to Enforce a Family Maintenance Order - [Section 44(1)(k)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(k) for the purpose of enforcing a maintenance order under *The Family Maintenance Act*;

Often information necessary to enforce a maintenance order cannot be collected directly from an individual who is 'in default' under a maintenance order, as he or she cannot be located or is resisting making the support payments under the order.

This clause 44(1)(k) complements subsections 55(2) and (2.1) of *The Family Maintenance Act*, which authorize a 'designated officer' under that Act to collect certain information from various sources, including government **departments**, agencies and other persons respecting:

- the whereabouts of a person who is entitled to receive, or who is required to make, payments under an order for spousal or child maintenance (support);
- the financial means, assets and liabilities of a person required to make payments under a maintenance order; etc.

Clause 44(1)(k) authorizes disclosure of additional **personal information** to the staff of the Maintenance Enforcement Office of Manitoba Justice if this information is necessary to enforce a maintenance order.

■ Disclosure Necessary to Protect Mental or Physical Health or Safety - [Clause 44(1)(l)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (l) where necessary to protect the mental or physical health or the safety of any individual or group of individuals;

Like other privacy laws, FIPPA permits disclosure of **personal information** to protect health and safety.

Clause 44(1)(l) permits disclosure of **personal information** where disclosure is

- necessary to protect the mental or physical health or safety of any individual including, but not limited to, the individual the **personal information** is about; or

- necessary to protect the mental or physical health or safety of a group of individuals.

"Safety" means the condition of being safe; freedom from danger or risks.[248]

For the clause to apply, there must be some potential threat, danger or harm to the mental or physical health or safety of an individual or group. Disclosure is "necessary" in the context of clause 44(1)(l) where the **public body** will be unable to properly or adequately protect the mental or physical health or safety of the individual or the group without disclosing the **personal information** in the proposed manner.

The decision to disclose must be made on a case by case basis, and the decision must be made carefully and sensitively. But, privacy laws do not stand in the way of a **public body** disclosing **personal information** where necessary to protect an individual or the public. In the words of the Ontario and B.C. Information and Privacy Commissioners, sometimes "life trumps privacy, and our laws reflect that reality".[249]

---

[248] *The Concise Oxford Dictionary, 9th Edition.*

[249] Practice Tool for *Exercising Discretion: Emergency Disclosure of Personal Information by*

Examples:

- Disclosure of **personal information** about a dangerous offender being released from a correctional institution through the Community Notification Advisory Committee process established by the Minister of Justice and Attorney General for Manitoba;

- Disclosure of information that a client of a **public body** is known to behave violently to **employees** to other **public bodies** and agencies that are likely to come into contact with this client, so appropriate precautions may be taken to protect their **employees** (such as arranging for the presence of a security guard, etc.).

Disclosure of personal health information to protect an individual or the public:

Under clause 22(2)(b) of *The Personal Health Information Act*, a trustee, including a **public body**, may disclose **personal health information** to any person if the trustee maintaining the information reasonably believes that disclosure is necessary to prevent or lessen a serious and immediate threat to:

- the health or safety of the individual the information is about or of another individual; or

- public health or safety.

Universities, Colleges and other Educational Institutions, October 2008, page 1. This joint paper of the Ontario and B.C. Information and Privacy Commissioners can be found on the Ontario Information and Privacy Commissioner's website at: http://www.oipc.bc.ca/tools-guidance/guidance-documents.aspx#

■ Disclosure to Comply with a Subpoena, Warrant or Order - [Clause 44(1)(m)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (m) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information or with a rule of court that relates to the production of information;

Clause 44(1)(m) permits a **public body** to disclose **personal information** in response to a properly authorized and served subpoena, warrant or order issued by a court or other person or body that is authorized to issue such documents.

To "comply" with a subpoena, warrant or order means to act in accordance with[250] or fulfill the requirements of the subpoena, warrant or order.

The word "subpoena" is from the Latin 'sub poena' – under penalty. A subpoena is also sometimes called a 'summons to witness'. A subpoena is a command issued at the request of a party to legal proceedings requiring attendance of the person named at a court or a hearing at a certain place and time to give testimony on a certain matter.[251] A subpoena may also require the person to bring records, documents, files and other specified information to the court or the hearing.

A "warrant" is an order of a judicial authority authorizing an officer named or described in the warrant to arrest a person, seize something (such as records), search something (such as a computer or premises) or execute or carry out some judicial sentence.[252]

---

250 *The Concise Oxford Dictionary, 9th Edition*.

251 *Black's Law Dictionary, 6th Edition*.

252 *The Dictionary of Canadian Law*.

An "order" is a direction of a court, judge, tribunal or official that commands a party to do or not to do something; a judgment, decree, direction or decision that is authorized or required to be made under a statute or regulation.[253]

Officials, bodies or tribunals who are not judges or courts only have authority to issue orders compelling attendance at a hearing or compelling production of documents or other information if that power is given to them by a statute or regulation. Examples of officials, bodies or tribunals who have been given such authority include:

- the Manitoba Labour Board,
- the Workers Compensation Board,
- a Commissioner appointed under Part 5 of *The Evidence Act* of Manitoba, etc.

Examples of rules of court that relate to the production of information include:

- the Court of Queen's Bench Rules respecting discovery of documents in a civil court proceeding;
- the common law rules developed by the criminal courts respecting Crown disclosure in criminal cases.

Although clause 44(1)(m) might appear to be permissive, as the term "may" is used, in reality a **public body** and its officers and **employees** normally comply with such documents both to assist in the administration of justice and because compliance is required by law. An officer or **employee** of a **public body** cannot ignore a subpoena, warrant or order, as he or she risks penalties – such as being cited for contempt by court and, at a minimum, fined – for doing so.

Time is usually important in responding to a subpoena, warrant or order to produce documents or information. A **public body** should consult with legal counsel immediately on receipt of a subpoena, warrant or order to determine:

- whether the document is properly authorized and drafted,
- whether the document has been properly served,

[253] *The Dictionary of Canadian Law*.

- whether the information required to be produced is legally compellable or whether there are some legal grounds for opposing the subpoena, warrant or order, and

- what information must be provided to comply with the subpoena, warrant or order.

Remember:

Clauses 3(c) and (d) of FIPPA state that FIPPA

> (c) does not limit the information otherwise available by law to a party to legal proceedings; and
>
> (d) does not affect the power of a court or tribunal to compel a witness to testify or to compel the production of documents.[254]

[254] Clauses 3(c) and (d) are discussed in Chapter 2, under *Procedures Not Affected by FIPPA*.

■ Disclosure for Legal Advice or Legal Services - [Clause 44(1)(n)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (n) for use in providing legal advice or legal services to the Government of Manitoba or the **public body**;

Clause 44(1)(n) recognizes that a **public body** may need to disclose **personal information** to legal counsel representing the **public body** or the Government of Manitoba for use in the day-to-day provision of legal advice or legal services or in the provision of legal advice or services respecting legal proceedings.

Clause 44(1)(n) applies to disclosure of **personal information** by a **department** or **government agency** to:

- Crown Counsel and Crown Prosecutors employed in the Manitoba Justice;
- to legal counsel on the staff of a **government agency** or a **local public body**; and
- to private bar legal counsel retained to act on behalf of the Government of Manitoba or the **public body**.

Clause 44(1)(n) applies where the legal advice or legal services are provided:

- to a **public body** (such as a **department**, a **government agency** or a **local public body**); or
- to the Government of Manitoba in the broad, 'corporate' sense.

  The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[255] and is a broader concept than **"department"** or **"public body"**.

[255] *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act*, C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

There is some overlap between clause 44(1)(n) and clauses 44(1)(o) (disclosure to enforce a legal right) and 44(1)(q) (disclosure for use in existing or anticipated legal proceedings).

■ Disclosure to Enforce a Legal Right - [Clause 44(1)(o)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(o) for the purpose of enforcing a legal right that the Government of Manitoba or the **public body** has against any person;

Clause 44(1)(o) permits a **public body** to disclose **personal information** to enforce a legal right of that **public body**, or of the Government of Manitoba, against any person.

"Person" means a natural person (a human being) and also includes a corporation and the heirs, executors, administrators or other legal representatives of a person.[256]

A "legal right" is a right based on a statute or regulation or on common law (that is, judge-made law).

Disclosure may be:

- to legal counsel (including Crown Counsel or Crown Prosecutors in Manitoba Justice, legal counsel on the staff of a **public body**, or private bar legal counsel retained by the **public body** or the Government of Manitoba); or

- to any person authorized to enforce the legal right of the **public body** or the Government of Manitoba (for example, a debt collection agency acting under a contract with the **public body** or the Government); etc.

[256] *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act*, C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

Clause 44(1)(o) does not permit a **public body** to disclose **personal information** to enforce the legal rights of another **public body**. For disclosure to be authorized under clause 44(1)(o), the legal right being enforced must be:

- a legal right of the **public body** that has custody or control of the **personal information**, as the phrase "the **public body**" is used in clause 44(1)(o); or

- a legal right of the Government of Manitoba in the broad, 'corporate' sense.

  The "Government of Manitoba" is "Her Majesty the Queen, acting for the Province of Manitoba".[257] The "Government of Manitoba" is a broader concept than the concept of **"department"** or **"public body"**.

There is some overlap between clauses 44(1)(o), 44(1)(n) and 44(1)(p).

[257] *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act*, C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

■ Disclosure to Determine the Amount of or Collect a Fine, Debt, Tax or Payment Owing or to Make a Payment - [Clause 44(1)(p)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(p) for the purpose of

(i) determining the amount of or collecting a fine, debt, tax or payment owing by an individual to the Government of Manitoba or to the **public body**, or to an assignee of either of them, or

(ii) making a payment;

1. Disclosure to determine the amount of or to collect a fine, debt, tax or payment owing to the Government of Manitoba or the public body, or an assignee of either of them - [Paragraph 44(1)(p)(i)]

Paragraph 44(1)(p)(i) permits a **public body** to disclose **personal information** for the purpose of determining the amount of or collecting a fine, debt, tax or payment owing if the fine, debt, tax or payment is:

(a) owing to the Government of Manitoba.

The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[258] and is a broader concept than **"department"** or **"public body"**.

In the government context, fines, debts, taxes and other amounts are usually owed to the Government or Manitoba in the broad 'corporate' sense, not to individual government **departments**.

[258] *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act*, C.C.S.M., c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

Amongst other things, clause 44(1)(p)(i) permits disclosure of **personal information** by one government **department** to another government **department** for the purpose of determining the amount of, or collecting, a fine, debt, tax or payment owing to the Government.

For example, the Department of Finance may disclose **personal information** to the Department of Education and Advanced Learning to enable Education and Advanced Learning to collect unpaid student loans owing to the Government of Manitoba.

*(b) owing to the **public body** that has custody or control of the **personal information** to be disclosed.*

Except as noted above, in the context of government **departments** and a fine, debt, tax or other payment owing to the Government of Manitoba, paragraph 44(1)(p)(i) does not permit a **public body** to disclose **personal information** for the purpose of determining the amount of, or collecting, a fine, debt, tax or payment owing to another **public body**, This is the effect of the phrase "the **public body**" in paragraph 44(1)(p)(i).[259]

For example, Manitoba Finance could not rely on clause 44(1)(p) to disclose **personal information** for the purpose of determining the amount of, or collecting, a fine, debt, tax or other amount owing to a municipality.

(c) *owing to an "assignee" of the Government of Manitoba or the **public body**.*

An "assignee" of the Government of Manitoba or of the **public body** is a person to whom the rights of the Government or the **public body** in the fine, debt, tax or payment have been transferred, usually by means of a written transfer document called an 'assignment'.[260]

---

[259] This provision is more limited than the corresponding provisions in the Alberta *Freedom of Information and Protection of Privacy Act* and the B.C. *Freedom of Information and Protection of Privacy Act*.

[260] *Black's Law Dictionary, 6th Edition*; *The Dictionary of Canadian Law*.

"Determining" the amount of a fine, debt, tax or payment owing means finding out or establishing[261] that amount.

"Collecting" a fine, debt, tax or payment owing occurs once a decision has been made by the **public body** that the individual owes the fine, debt, tax or payment and the **public body** intends to seek payment of the amount owing.

A "fine" is a sum of money ordered to be paid to the Government of Manitoba or a **public body** (such as a municipality) by an offender, as punishment for an offence.[262]

A "debt" is a specified amount of money due to the Government of Manitoba or due to the **public body** that has custody or control of the **personal information** to be disclosed, and includes not only the obligation of the debtor to pay but also the right of the creditor to receive and enforce the payment.[263]

A "tax" is "a contribution to state revenue compulsorily levied on individuals, property or businesses",[264] and includes federal, provincial, municipal and school taxes.

The phrase "payment owing" is broad and includes amounts that are payable to the Government of Manitoba or to the **public body** that has custody or control of the **personal information** to be disclosed – for example, unpaid license fees, etc.

261 *The Concise Oxford Dictionary, 9th Edition.*

262 *The Dictionary of Canadian Law*.

263 *The Dictionary of Canadian Law*; *Black's Law Dictionary, 6th Edition*.

264 *The Concise Oxford Dictionary, 9th Edition*.

Remember:

When a **public body** provides **personal information** to a collection agency it has hired to collect fines, debts, taxes or other payments owing to the **public body**, this is a "use" – not a disclosure – of the **personal information** as the collection agency is providing services to, and acting on behalf of, the **public body**. The **public body** remains responsible for the **personal information**.[265]

2. Making a payment [Paragraph 44(1)(p)(ii)]

A "payment" in the context of paragraph 44(1)(p)(ii) is a sum of money that the Government of Manitoba or a **public body** owes to someone.

Paragraph 44(1)(p)(ii) permits a **public body** to disclose **personal information** "for the purpose of … making a payment". This situation will most commonly arise when a **public body** or the Government of Manitoba owes an individual money and

- the individual has moved and the **public body** does not have a forwarding address; or
- the **public body** is trying to verify the identity of the individual so it can make the payment.

[265] "Use" of personal information is discussed earlier in this Chapter, under *Use of Personal Information*. The responsibility of **public bodies** for **personal information** dealt with by its contractors and agents is discussed earlier in this Chapter, under *Accountability and Employees, Contractors and Agents*.

■ Disclosure for Use in Legal Proceedings - [Clause 44(1)(q)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(q) for use in existing or anticipated legal proceedings to which the Government of Manitoba or the **public body** is a party;

Clause 44(1)(q) allows a **public body** to disclose **personal information** for use in:

- existing legal proceedings to which the Government of Manitoba or the **public body** is a party; or
- anticipated legal proceedings to which the Government of Manitoba or the **public body** is a party.

A "legal proceeding" is any civil or criminal proceeding or inquiry in which evidence is or may be given, and includes an arbitration;[266] any proceeding authorized or sanctioned by law, and brought or instituted, for the acquiring of a right or the enforcement of a remedy.[267] "Legal proceedings" are proceedings before a court, tribunal or other body that has authority, by law or consent, to make decisions about a person's rights.

Clause 44(1)(q) applies where:

- the **public body** disclosing the **personal information** is a party to the existing or anticipated legal proceedings; or
- the Government of Manitoba, in the broad 'corporate' sense, is a party to the existing or anticipated legal proceedings.

266 *The Dictionary of Canadian Law.*

267 *Black's Law Dictionary, 6th Edition.*

> The Government of Manitoba is "Her Majesty the Queen, acting for the Province of Manitoba,"[268] and is a broader concept than **"department"** or **"public body"**. Usually, legal proceedings involving a **department** or **departments** of the government are brought against "The Government of Manitoba" and not against the individual **departments**.[269]

Disclosure may be

- to legal counsel acting for the **public body** or the Government (including Crown Counsel or Crown Prosecutors in Manitoba Justice, staff legal counsel or private bar legal counsel retained by the **public body** or the Government); or

- to persons assisting counsel in preparing for or conducting the legal proceedings on behalf of the **public body** or the Government of Manitoba, including experts, investigators, etc.

There is some overlap between clause 44(1)(q) and clauses 44(1)(n) (disclosure for use in providing legal advice or legal services) and 44(1)(o) (disclosure to enforce a legal right).

---

[268] *The Interpretation Act* of Manitoba, section 17 and the Schedule of Definitions. *The Interpretation Act*, C.C.S.M. c. I80, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

[269] *The Proceedings Against the Crown Act*, C.C.S.M. c. PI40, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p140e.php.

■ Disclosure for Law Enforcement Purposes or Crime Prevention - [Clause 44(1)(r)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (r) for **law enforcement** purposes or crime prevention;

Clause 44(1)(r) permits disclosure of **personal information** by a **public body** for either of two purposes:

(i) **law enforcement** purposes; or

(ii) crime prevention.

1. Meaning of "Law enforcement"[270]

"Law enforcement" is defined in subsection 1(1) of FIPPA:

> **"law enforcement"** means any action taken for the purpose of enforcing an **enactment**, including
>
> (a) policing,
>
> (b) investigations or inspections that lead or could lead to a penalty or sanction being imposed, or that are otherwise conducted for the purpose of enforcing an **enactment**, and
>
> (c) proceedings that lead or could lead to a penalty or sanction being imposed, or that are otherwise conducted for the purpose of enforcing an **enactment**;

[270] The definition **"law enforcement"** is discussed in Chapter 2, under *Key Definitions*.

"Law enforcement" is not limited to the investigative activities of police forces, but also includes a wide variety of investigations and actions by **public bodies**, if they are undertaken for the purpose of enforcing an **enactment**.

"Enactment" is defined in subsection 1(1) of FIPPA as "an Act or regulation". For the purposes of clause 44(1)(r),

- An "Act" is a statute passed by the Legislative Assembly of a province or by the Parliament of Canada.

- A "regulation" is a law made under the authority of a statute by the Lieutenant Governor in Council (in the case of a province), the Governor General in Council (in the case of Canada), a minister, etc.

Examples of **law enforcement** include:

- investigations under the *Controlled Drugs and Substances Act* (Canada);
- safety inspections under *The Workplace Safety Act;*
- investigations by the Office of the Fire Commissioner;
- the regulatory activities of the Superintendent of Insurance;
- investigations under *The Human Rights Code* of Manitoba;
- investigations by child and family services agencies to determine if a child is in need of protection under *The Child and Family Services Act*; etc.

This list is by no means exhaustive, and illustrates the broad range of activities that may be **law enforcement** for the purposes of FIPPA.

2. Meaning of "Crime Prevention"

"Crime prevention" is prevention of conduct that society's laws prohibit.[271]

[271] Definition of "crime" from *The Dictionary of Canadian Law.*

3. Discretion to disclose

Clause 44(1)(r) is intended to permit sharing of **personal information** among **public bodies** to enable **law enforcement** activities to be properly carried out and to enable **law enforcement** agencies and other **public bodies** to prevent criminal activities.

A **public body** has a discretion under clause 44(1)(r) to disclose or not to disclose **personal information** for **law enforcement** purposes or crime prevention and should be cautious when the person or agency requesting the information seems to be on a 'fishing expedition' and cannot provide definite and focused information as to the nature of the investigation and why the requested **personal information** is necessary.

Personal information should generally not be disclosed by a **public body** under clause 44(1)(r) on the basis that there is a vague suspicion, surmise or guess that it might be useful for **law enforcement** purposes or crime prevention.

A **public body** that receives a request for **personal information** for **law enforcement** purposes should:

- confirm the nature of the **law enforcement** action – for example, by confirming that there is an actual investigation, not just the possibility of an investigation in the future;
- confirm the legal authority for the **law enforcement** action;
- determine the exact nature of the **personal information** requested, and the purpose for which it will be used;
- keep in mind the **public body's** duty under subsection 42(2) of FIPPA to disclose only the minimum amount of **personal information** necessary to accomplish the **law enforcement** purpose.

A **public body** should consider consulting with legal counsel when it receives a request for **personal information** for **law enforcement** purposes or crime prevention.

■ Disclosure Among Law Enforcement Agencies - [Clause 44(1)(s)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (s) if the **public body** is a **law enforcement** agency and the information is disclosed to
>
> (i) another **law enforcement** agency in Canada, or
>
> (ii) a **law enforcement** agency in a foreign country under an arrangement, written agreement, treaty or legislative authority;

Clause 44(1)(s) only applies to **public bodies** that are **law enforcement** agencies. It permits a Manitoba **law enforcement** agency to disclose **personal information** to other **law enforcement** agencies in Manitoba and to **law enforcement** agencies outside Manitoba.

1. What is a law enforcement agency?

Under clause 44(1)(s), disclosure is authorized by one **law enforcement** agency to another **law enforcement** agency.

"Law enforcement" is defined in subsection 1(1) of FIPPA.[272]

A "**law enforcement** agency" means an agency primarily engaged in:

- enforcing an **enactment** (that is, a statute or a regulation);
- policing;
- investigations or inspections that could result in a penalty or sanction being imposed or that are otherwise conducted for the purpose of enforcing an **enactment** ; or

[272] The definition **"law enforcement"** is discussed in Chapter 2, under *Key Definitions*.

- proceedings that could result in a penalty or sanction being imposed or that are otherwise conducted for the purpose of enforcing an **enactment**.

Examples of **law enforcement** agencies include, but are not limited to:

- the Winnipeg Police Service;
- the Manitoba Securities Commission;
- conservation officers enforcing *The Conservation Act*;
- the office of the Chief Fire Commissioner;
- public health inspectors enforcing *The Public Health Act*; etc.

This list of **law enforcement** agencies is by no means exhaustive; it is intended to emphasize the broad range of entities that may be **law enforcement** agencies.

2. Disclosure to another law enforcement agency in Manitoba or Canada [Paragraph 44(1)(s)(i)]

Paragraph 44(1)(s)(i) permits a Manitoba **public body** that is a **law enforcement** agency to disclose **personal information**

(i) to another **law enforcement** agency in Manitoba; and

(ii) to Canadian federal, provincial and municipal **law enforcement** agencies.

This includes, but is not limited to, disclosure to:

- the Winnipeg Police Service;
- the RCMP and other provincial and municipal police forces;
- Revenue Canada;
- safety and health inspection officers enforcing safety and health legislation;

- fire commissioners' offices enforcing fires prevention legislation;
- Human Rights Commissions enforcing human rights legislation; etc.

Again, this list of **law enforcement** agencies is by no means exhaustive; it is intended to emphasize the broad range of **law enforcement** agencies to which **personal information** may be disclosed under this paragraph.

3. Disclosure to a law enforcement agency in a <u>foreign country</u> - [Paragraph 44(1)(s)(ii].

Paragraph 44(1)(s)(ii) permits a Manitoba **public body** that is a **law enforcement agency** to disclose **personal information** to police forces and other law enforcement agencies in other countries.

Disclosures under this paragraph must be made in accordance with an arrangement, written agreement, treaty or legislative authority.

An "arrangement" is a settlement of mutual relations or claims between parties;[273] an arrangement may or may not be in writing.

An "agreement" is a mutual understanding, an arrangement between parties as to a course of action,[274] a contract.[275] An agreement is more precise than an arrangement. For the purposes of paragraph 44(1)(s)(ii) an agreement respecting disclosure of **personal information** to a foreign **law enforcement** agency must be in writing.

[273] *The Compact Edition of the Oxford English Dictionary*.

[274] *The Concise Oxford Dictionary, 9th Edition*.

[275] *The Dictionary of Canadian Law*.

A "treaty" is a compact made between two or more independent nations with a view to the public welfare,[276] a binding agreement between states.[277]

"Legislative authority" means that the disclosure of **personal information** is authorized by some statute or regulation other than FIPPA.

A **public body** that is a **law enforcement** agency has a discretion under clause 44(1)(s) to disclose or not to disclose **personal information** to another **law enforcement** agency. In the absence of a requirement in some other legislation or in an agreement or treaty, a Manitoba **law enforcement** agency should be cautious about disclosing **personal information** when the person or agency requesting it seems to be on a 'fishing expedition' and cannot provide definite and focused information as to the nature of the investigation and why the requested information is necessary for the investigation.

It is recommended that **public bodies** consult with legal counsel before relying on clause 44(1)(s).

[276] *Black's Law Dictionary, 6th Edition*.

[277] *The Dictionary of Canadian Law*.

■ Disclosure for the Purpose of Supervising an Individual in Custody - [Clause 44(1)(t)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (t) for the purpose of supervising an individual in the custody of or under the control or supervision of a correctional authority;

Clause 44(1)(t) permits disclosure of **personal information** for the purpose of supervising an individual who is:

(i) in the custody of a correctional authority; or

(ii) under the control or supervision of a correctional authority.

Custody

'Custody' may mean actual imprisonment or physical detention or the power, legal or physical, to imprison or take manual possession.[278]

Examples of persons who are in the custody of a correctional authority include:

- persons who are detained in custody under a federal or provincial statute or a municipal bylaw;
- persons remanded in custody by a court, who are charged but not yet found guilty or are not yet sentenced;
- young persons detained in open or secure custody, or who are in pre-trial detention, under the *Youth Criminal Justice Act (Canada)*;
- parole violators detained in custody under a warrant issued by a parole board.

[278] *Black's Law Dictionary, 6th Edition*.

Control or Supervision

'Supervision' means having general oversight or superintendence over a person.[279]

Adults and young persons who are subject to control by a correctional authority or its agents due to legally imposed restrictions on their liberty are "under the control or supervision of a correctional authority".

Examples include:

- persons on parole;
- persons on probation;
- persons on a temporary absence permit;
- persons under bail supervision;
- persons performing community service work under a court order.

[279] *Black's Law Dictionary, 6th Edition.*

■ Disclosure Necessary for the Security of a Correctional Institution - [Clause 44(1)(u)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (u) where disclosure is necessary for the security of a correctional institution;

"Correctional institution" means a place of lawful detention; a “custodial facility” under *The Correctional Services Act*.[280]

“Security” generally means a condition of safety from attack or danger[281] or a state of physical integrity.

The security of a correctional institution includes the safety of the occupants as well as the integrity of the physical structure and the security of adjoining or connecting structures.

---

[280] *The Correctional Services Act*, C.C.S.M. c. C230, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/c230e.php.

[281] *The Concise Oxford Dictionary, 9th Edition.*

■ Transfer to the Archives of Manitoba or to the Archives of the Public Body - [Clause 44(1)(v)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (v) by transfer to the Archives of Manitoba or to the archives of the **public body** for records management or archival purposes;

Clause 44(1)(v) permits the transfer of **records** containing **personal information** to:

- the Archives of Manitoba, or
- in the case of a **public body** that has its own archives, to the archives of the **public body**.

for "records management or archival purposes".

The Archives of Manitoba is governed by *The Archives and Recordkeeping Act*.[282]

Some **local public bodies** have their own archives – for example, the University of Manitoba and The City of Winnipeg.

"Records management or archival purposes" include:

- storage, retrieval and destruction of **records**;
- conservation, reformatting and treatment of **records**;
- **records** description and arrangement;
- **records** inspection and monitoring; etc.

This provision does not authorize transfer of **records** in the custody and control of a **public body** that contain **personal information** to a private archives.

---

[282] *The Archives and Recordkeeping Act*, C.C.S.M. c. A132 can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/a132e.php.

Note:

Clause 4(j) of FIPPA states that FIPPA does not apply to **records** that are acquired by the Archives of Manitoba, or by the archives of a **public body**, from a person or entity that is not a **public body**.[283]

[283] Clause 4(j) of FIPPA, discussed in Chapter 2, under *Records That Do Not Fall under FIPPA*. Bodies that fall under FIPPA are discussed in Chapter 2, under *Public Bodies that Fall Under FIPPA*.

■ Disclosure to an Officer of the Legislature - [Clause 44(1)(w)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(w) to an officer of the Legislature, if the information is necessary for the performance of the duties of that officer;

"Officer of the Legislature" has the same meaning as **"officer of the Legislative Assembly"** (defined in subsection 1(1) of FIPPA):

- the Speaker of the Legislative Assembly, elected by the members of the Assembly under *The Legislative Assembly Act*,
- the Clerk of the Legislative Assembly, appointed under *The Legislative Assembly Management Commission Act*,
- the Chief Electoral Officer, appointed under *The Elections Act,*
- the **Ombudsman**, appointed under *The Ombudsman Act,*
- the Children's Advocate, appointed under *The Child and Family Services Act*,
- the Manitoba Auditor General, appointed under *The Auditor General Act,*
- the Information and Privacy **Adjudicator**, appointed under FIPPA,[284] and
- the commissioner appointed under *The Legislative Assembly and Executive Council Conflict of Interest Act*.

[284] The appointment and role of the Information and Privacy Adjudicator is discussed in Chapter 8 of this Manual.

Disclosure is permitted to any of these officers under clause 44(1)(w) if the **personal information** is necessary for the performance of their duties. "Necessary" in this context means that the officer will be unable to properly or fully carry out his or her responsibilities without the **personal information** – that is, the officer must 'need to know' the **personal information** to carry out his or her responsibilities as an officer of the Legislature.

■ Disclosure to an Expert Under Clause 24(b) - [Clause 44(1)(x)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(x) to an expert for the purposes of clause 24(b)*;*

Disclosure harmful to individual or public safety
24 The **head** of a **public body** may refuse to disclose to an **applicant** information, including **personal information** about the **applicant**, if disclosure could reasonably be expected to

(b) result, in the opinion of a duly qualified physician, psychologist, or other appropriate expert, in serious harm to the **applicant's** mental or physical health or safety;

Clause 44(1)(x) only applies where there has been a request for access to a **record** in the custody or under the control of a **public body** under Part 2 of FIPPA (Access to Information) and the **head** of the **public body** is considering relying on the exception to disclosure in clause 24(b) of FIPPA as a basis for refusing access.[285] It allows the **public body** to fulfill its obligations under clause 24(b) of FIPPA.

Clause 44(1)(x) permits a **public body** to disclose **personal information** to a duly qualified physician, psychologist, or other appropriate expert so that the expert can provide an opinion to the **public body** as to whether disclosure of information to an **applicant** requesting access to **records** under Part 2 of FIPPA could reasonably be expected to result in serious harm to the **applicant's** mental or physical health or safety.

[285] Section 24 is discussed in Chapter 5, under *Exceptions to Disclosure: Disclosure harmful to individual health or safety or public safety*.

■ Disclosure of Business Contact Information - [Clause 44(1)(x.1)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(x.1) if the **personal information** is information of a type routinely disclosed in a business or professional context, and the disclosure

(i) is limited to the individual's name, position name or title, business address, telephone number, facsimile number and e-mail address, and

(ii) does not reveal other **personal information** about the individual or **personal information** about another individual;[286]

Clause 44(1)(x.1) permits a **public body** to disclose the name and business contact information of individuals, as long as doing so will not disclose other **personal information** about the individual, or **personal information** about any other individual.

Four conditions must be met:

(i) The information to be disclosed must be information of a type routinely disclosed in a business or professional context;

[286] This provision was added to FIPPA by *The Freedom of Information and Protection of Privacy Amendment Act*, S.M. 2008 c. 40. The amending Act can be found at: http://web2.gov.mb.ca/laws/statutes/2008/c04008e.php.

(ii) The information to be disclosed must be limited to the individual's

- name,
- position name or title,
- business address,
- business telephone number,
- business facsimile number, and
- business e-mail address.

This is the information that would usually appear on an individual's business card.

(iii) The information disclosed must not reveal other **personal information** about the individual.

(iv) The information disclosed must not reveal **personal information** about another individual.

Example:

A **public body** may provide a list of the business participants in a consultation process respecting proposed business legislation.

■ Disclosure to a Relative in the Case of Injury, Illness or Death - [Clause 44(1)(y)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(y) for the purpose of

(i) contacting a relative or friend of an individual who is injured, incapacitated or ill,

(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 in the circumstances, of the individual's death;

Clause 44(1)(y) permits a **public body** to disclose **personal information** in certain limited compassionate circumstances.[287]

Disclosure of **personal information** is permitted:

(i) for the purpose of contacting a relative or friend of an individual who is injured, incapacitated or ill;

A "relative" is an individual connected with another by blood or affinity (that is, by reason of marriage).[288] For the purpose of clause 44(1)(y)(i), "relative" includes a spouse, common-law spouse, children, parents, siblings or anyone else who can establish a familial relationship with the individual.

[287] Disclosure of **personal health information** for compassionate reasons is addressed in clause 22(2)(c) of *The Personal Health Information Act*; disclosure of limited **personal health information** about a patient or resident in a health care facility to family members is addressed in section 23 of *The Personal Health Information Act*.

[288] *Black's Law Dictionary, 6th Edition*.

This provision does not permit disclosure of the nature of the illness or injury or of the cause of death; such information is **personal health information** and can only be disclosed in accordance with *The Personal Health Information Act*.[289]

(ii) for the purpose of assisting in identifying a deceased individual; or

(iii) for the purpose of informing the representative or a relative of a deceased individual, or any other person it is reasonable to inform in the circumstances, of the individual's death.

The "representative" of a deceased individual is the executor named in the will of the deceased individual or, where there is no will, the administrator appointed by a court to administer the estate of the deceased individual.

A "relative" is an individual connected with another by blood or affinity (that is, by reason of marriage).[290] For the purposes of clause 44(1)(y)(iii),"relative" includes a spouse, common-law spouse, children, parents, siblings or anyone else who can establish a familial relationship with the deceased individual.

---

289 *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

290 Black's Law Dictionary, 6th Edition.

■ Disclosure to a Relative of a Deceased Individual - [Clause 44(1)(z)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (z) to a relative of a deceased individual if the **head** of the **public body** reasonably believes that disclosure is not an unreasonable invasion of the deceased's privacy;

Clause 44(1)(z) permits a **public body** to disclose **personal information** about a deceased individual to a relative if the **head** of the **public body**, or his or her delegate, reasonably believes that disclosure is not an unreasonable invasion of the deceased's privacy.

Personal health information about a deceased individual can be disclosed to a relative on a similar basis under clause 22(2)(d) of *The Personal Health Information Act*.[291]

These provisions recognize that there is often a lessening of privacy concerns with the passage of time after the death of an individual and that a relative may have a legitimate need to obtain **personal information** about the deceased individual.

Personal information in a **record** is normally protected for a period of 100 years (section 48 of FIPPA). Where there is a request for access under Part 2 of FIPPA, the privacy of a deceased individual is protected for 10 years (clause 17(4)(h)). Clause 44(1)(z) permits earlier disclosure of **personal information** about a deceased individual to a relative, provided disclosure is not an unreasonable invasion of the deceased's privacy.

[291] *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

A "relative" is an individual connected with another by blood or affinity (that is, by reason of marriage);[292] for the purpose of clause 44(1)(z) "relative" includes a spouse, common-law spouse, children, parents, siblings or anyone else who can establish a familial relationship with the deceased individual.
Before disclosing **personal information** under clause 44(1)(z), the **head** of the **public body**, or his or her delegate, must believe that disclosure to the requesting relative "is not an unreasonable invasion of the deceased's privacy". In determining whether or not disclosure would be an "unreasonable invasion of the deceased's privacy", the **head** should balance the sensitivity of the information (including any known wishes of the deceased individual) against the interest of the relative in knowing the information. Ordinarily, if the information is sensitive, the interest of the relative should go beyond mere curiosity.

Proof of the relationship with the deceased individual must be provided before **personal information** is disclosed under clause 44(1)(z). The **public body** must also be satisfied that the individual the information is about is in fact dead.

A relative of a deceased individual who is refused information under clause 44(1)(z) may make a **complaint** to the Ombudsman about the refusal [subsection 59(4)].[293]

[292] *Black's Law Dictionary, 6th Edition*.

[293] Subsection 59(4) of FIPPA and complaints to the Ombudsman are discussed in Chapter 8 of this Manual.

■ Disclosure to an Information Manager - [Clause 44(1)(aa)]

Clause 44(1)(aa) of FIPPA permits a **public body** to disclose **personal information** to an **"information manager"**, if the requirements in section 44.1 of FIPPA are met.

Section 44.1 is discussed later in this Chapter, under *Information Managers*.

■ Disclosure of Information Available to the Public - [Clause 44(1)(bb)]

> **Disclosure of personal information**
> **44(1)** A **public body** may disclose **personal information** only
>
> (bb) when the information is available to the public;

Clause 44(1)(bb) permits a **public body** to disclose **personal information** when the information is available to the public. The clause applies, for example, to information that has been published or that constitutes or is part of a **record** that is publicly available (for example, through a public registry).

In applying this clause, however, it is important that the **public body** assess how public the information really is. Factors such as the circumstances in which the information was released to the public or the media, when it was released, and how much information is properly in the public realm will be relevant.

For example, a **public body** should not automatically treat **personal information** about an individual as public and freely disclose it to others simply because the information has been published in some form in the media or in a report that has been made public. Depending on the circumstances of the publication, further disclosure may result in an unreasonable invasion of the individual's privacy – and may even expose the **public body** to legal liability (e.g. to a civil suit for defamation).

Before relying on this clause as authority to disclose **personal information**, it is strongly recommended that legal counsel be consulted.

■ Disclosure under Section 47 (Research Purposes) or Section 48 (Record More than 100 Years Old) - [Clause 44(1)(cc)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(cc) in accordance with section 47 or 48.

A **public body** may also disclose **personal information** where:

- the disclosure is for a research purpose and is approved by the **head** of the **public body** in accordance with the requirements of section 47 of FIPPA;
- the **record** is more than 100 years old [section 48].

Sections 47 and 48 are discussed later in this Chapter.

A note about the former section 46

As of January 1, 2011, FIPPA was amended to repeal (that is, remove) the former section 46. Section 46 provided a process whereby a **public body** could disclose **personal information** on a bulk basis, or use or disclose **personal information** for data linkage or data matching purposes, where the use or disclosure was not authorized under any other provision of FIPPA. The process included a review of the proposed request for use or disclosure, with recommendations, by a government review committee. Section 46 created a category of permitted uses and disclosures in addition to those set out in sections 43 and 44 of FIPPA; it was unique to Manitoba, and was not often relied on.

Since the former section 46 has been repealed (that is, removed from FIPPA), **public bodies** can no longer rely on it as authority to disclose **personal information**.

Recognizing that, in the past, a **public body** and a private sector organization may have, in good faith, relied on section 46 to enter into an agreement, the amendments that repeal section 46 of FIPPA also contain two 'saving' provisions.

Right to disclose to War Amps preserved

97.1(1) If a **public body**, pursuant to an agreement entered into under section 46 before the coming into force of this section, disclosed names, addresses and drivers' licence numbers to the War Amputations of Canada, the **public body** may continue to disclose that information despite subsection 44(1) (restrictions on disclosure), if War Amputations of Canada uses the information only in accordance with the terms of the agreement.

Local public bodies

97.1(2) If a **local public body** disclosed information pursuant to an agreement entered into under section 46 before the coming into force of this section, it may continue to do so despite subsection 44(1) (restrictions on disclosure), if the body to whom the information is disclosed uses it only in accordance with the terms of the agreement.[294]

[294] Section 46 was repealed by *The Freedom of Information and Protection of Privacy Amendment Act*, S.M. 2008 c. 40. The amending Act is in effect as of January 1, 2011, and can be found at: http://web2.gov.mb.ca/laws/statutes/2008/c04008e.php.

■ Disclosure by an Education Institution for Fundraising - [Clause 44(1)(dd)]

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(dd) if the **public body** is an educational institution and the disclosure is for the purpose of fundraising activities of the educational institution, but only if

(i) the disclosure is of information in the alumni **records** of the educational institution and is reasonably necessary for the fundraising activities, and

(ii) the educational institution and the persons to whom the information is disclosed have entered into a written agreement that complies with subsection (1.1).

Fundraising agreement
44(1.1) An agreement between an educational institution and another person to permit disclosure of **personal information** under this section must

(a) require that when individuals are first contacted for the purpose of soliciting funds and periodically afterwards, they are informed of their right to request that their **personal information** cease to be disclosed;

(b) allow individuals, on request, a right of access to **personal information** that is disclosed about them under clause (1)(dd); and

(c) require that the person to whom the information is disclosed cease to use the **personal information** of any individual who so requests.[295]

[295] This new permitted disclosure was added to FIPPA by *The Freedom of Information and Protection of Privacy Amendment Act*, S.M. 2008 c. 40. The amending Act can be found at: http://web2.gov.mb.ca/laws/statutes/2008/c04008e.php.

(i) These new provisions only apply to an "educational institution".

The term “educational institution” is not defined in FIPPA, but would include a school, community college, university, college, etc. The University of Manitoba and Red River College are examples of “educational institutions”.

(ii) The disclosure is permitted only for the purpose of fundraising activities carried out by or on behalf of the educational institution that is disclosing the **personal information**.

For example, the provision does not authorize an educational institution to disclose **personal information** about alumni (without their consent) to a charitable organization to assist the charitable organization in its fundraising activities.

(iii) The disclosure is limited to information in the alumni **records** of the educational institution.

(iv) The information disclosed from the institution's alumni **records** must be "reasonably necessary" for the fundraising activities.

(v) The educational institution and the organization or person receiving the alumni information for fund raising purposes must enter into a written agreement that complies with subsection 44(1.1) of FIPPA.

(vi) The written agreement must include provisions that:

(a) require individuals to be informed of their right to request that their **personal information** cease to be disclosed, when they are first contacted for the purpose of soliciting funds and periodically afterwards;

That is, the individual must be given notice of his or her right under clause 44(1.1)(c) of FIPPA to request that his or her **personal information** not be used for this purpose.

(b) allow individuals, on request, a right of access to the **personal information** that is disclosed about them; and

(c) require that the person to whom the information is disclosed cease to use the **personal information** of any individual who so requests.

That is, the individual the information is about has the right to 'opt out' – to request that the organization or person that has received his or her **personal information** cease to use it.

In keeping with the "Openness" privacy principles, educational institutions that plan to rely on these provisions may want to consider taking steps to inform their alumni about them, and of the right to request that their **personal information** not be disclosed or used for these purposes.

INFORMATION MANAGERS - [SUBSECTION 1(1), CLAUSE 44(1)(AA) & SECTION 44.1]

Each **public body** that falls under FIPPA is responsible for the **personal information** in its custody or under its control, and for ensuring that its **employees** – that is, its officers, staff, contractors and agents – comply with FIPPA.[296] A **public body** cannot avoid its responsibility to deal with and protect **personal information** as required by FIPPA by contracting with a service provider, etc.

An **information manager** is a particular type of service provider. Subsection 1(1) of FIPPA defines **"information manager"**, and section 44.1 of FIPPA sets out the protection of privacy requirements that must be met when a **public body** proposes to contract with an **information manager** to deal with **personal information** on the **public body's** behalf.[297]

The definition of **"information manager"**, and the requirements in section 44.1 of FIPPA, are substantially the same as the information manager definition and provisions in *The Personal Health Information Act*.[298]

---

[296] This responsibility is discussed earlier in this Chapter, under *Accountability and Employees, Contractors and Agents*.

[297] The definition "information manager" and section 44.1 were added to FIPPA by *The Freedom of Information and Protection of Privacy Amendment Act*. The amending Act can be found at: http://web2.gov.mb.ca/laws/statutes/2008/c04008e.php.

[298] Section 25 of *The Personal Health Information Act* sets out the requirements that must be met, including the requirement for a written agreement, where a trustee (including a **public body**) discloses **personal health information** to an 'information manager' for the purpose of processing, storing or destroying the information or providing the trustee with information management or information technology services. *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

Disclosure of personal information
44(1) A **public body** may disclose **personal information** only

(aa) to an information manager in accordance with section 44.1;

Public body may provide information to an information manager
44.1(1) A **public body** may provide **personal information** to an **information manager** for the purpose of processing, storing or destroying it or providing the public body with information management or information technology services.

Restrictions on use
44.1(2) An **information manager** may use **personal information** provided to it under this section only for the purposes and activities mentioned in subsection (1), which must be purposes and activities that the **public body** itself may undertake.

Agreement required
44.1(3) A **public body** that wishes to provide **personal information** to an **information manager** under this section must enter into a written agreement with the **information manager** that provides for the protection of the **personal information** against such risks as unauthorized access, use, disclosure, destruction or alteration, in accordance with the regulations.

Information manager shall comply with Act
44.1(4) An **information manager** shall comply with

(a) the same requirements concerning the protection of **personal information** that the **public body** is required to comply with under this Act: and

(b) the duties imposed on the **information manager** under the agreement entered into under subsection (3).

Offences
85(1) Any person who wilfully

(e) fails to comply with subsection 44.1(4) (obligations of an **information manager**);

is guilty of an offence and liable on summary conviction to a fine of not more than $50,000.

PROTECTION OF PRIVACY: INFORMATION MANAGERS
CLAUSE 44(1)(AA) AND SECTION 44.1

1. What is an 'information manager'?

An "information manager" is a specific type of contractor or agent:

> **1(1)** **"information manager"** means a person or body that
>
> (a) processes, stores or destroys personal information for a **public body**, or
>
> (b) provides information management or information technology services to a **public body**;

Examples of 'information managers' include contractors and agents:

- that provide off-site **records** storage for a **public body**;
- that provide off-site **record** destruction services to a **public body**;
- that provide electronic information management services to a program, **department**, **government agency** or the government;
- that provide information technology services – such as technology support services respecting an information management system – to a program, **department**, **government agency** or the government; etc.

2. Requirements respecting information managers

Section 44.1 of FIPPA sets out the protection of privacy requirements that a **public body** and its **information manager** must meet. This includes entering into a written agreement that properly protects **personal information**.

(i) A **public body** is authorized to provide **personal information** to an **information manager** only if <u>all</u> the requirements in subsections 44.1(1), (2) and (3) of FIPPA are met.

(ii) These requirements apply whenever a public body provides **personal information** to an organization or entity that falls within the definition **"information manager"** in FIPPA.

That is, the requirements in subsection 44.1 apply if the organization or entity will:

- process, store or destroy **personal information** for the **public body**; or
- provide information management or information technology services to the **public body**.

If there is any question as to whether a contractor or agent is an **"information manager"**, contact legal counsel.

(iii) A **public body** is authorized to provide **personal information** to an **information manager** only for the purpose of:

- processing, storing or destroying the **personal information**; or
- providing information management or information technology services to the **public body** [subsection 44.1(1)].

(iv) A **public body** cannot contract with an **information manager** to do something that the **public body** itself could not do [subsection 44.1(2)].

(v) An **information manager** can only use the **personal information** provided to it for the purposes of:

- processing, storing or destroying the **personal information** for the **public body**; or
- providing information management or information technology services to the **public body**.

The **information manager** cannot use the **personal information** for any other purposes. (This restriction needs to be clearly set out in the agreement between the **public body** and the **information manager**.)

(vi) The **public body** and the **information manager** must enter into a written agreement that provides for the protection of the **personal information** against such risks as unauthorized access, use, disclosure, destruction or alteration [subsection 44.1(3)].

This requirement is discussed below. It is strongly recommended that legal counsel be consulted when developing and negotiating an information management agreement with an **information manager**.

(vii) FIPPA states that the **information manager** must comply with:

- the same requirements concerning the protection of **personal information** that the **public body** is required to comply with under FIPPA; and

- the duties imposed on the **information manager** under the agreement with the **public body** [subsection 44.1(4)].

This means that an **information manager** has duties and obligations not only under the agreement with the **public body**, but also under FIPPA itself.

An **information manager** may be committing an offence under FIPPA if it wilfully fails to comply with its duties and obligations under the contract or its duties and obligations under FIPPA. If the **information manager** is found guilty of an offence under FIPPA by a court, the information manager may be required to pay a fine of up to $50,000.[299]

(viii) **Personal information** that has been provided to an **information manager** under an information management agreement with a **public body** is deemed to be in the custody and control of the **public body** for the purposes of FIPPA [subsection 44.1(5)].

In other words, the access to information and protection of privacy provisions of FIPPA apply to this information even if it is held by the **information manager**, and the **public body** continues to be responsible and accountable for it.

[299] Clause 85(1)(e) of FIPPA.

3. The information management agreement [Subsection 44.1(3)]

It is strongly recommended that legal counsel be consulted to assist in developing and negotiating an information management agreement that will meet the requirements of section 44.1 of FIPPA. The following very general comments do not take the place of specific legal advice and assistance.

The Lieutenant Governor in Council may make regulations respecting the required information management agreement under subsection 44.1(3) of FIPPA, but, at present there are no such regulations.[300]

Subsection 44.1(3) of FIPPA identifies some of the risks that must be addressed in an information management agreement. The agreement must include provisions that protect the **personal information** provided to the **information manager** from "such risks as unauthorized access, use, disclosure, destruction or alteration".[301]

(i) Unauthorized access

'Unauthorized access' to **personal information** occurs whenever an officer, employee or agent of the **information manager** has access to **personal information** that he or she does does not need to see or handle in the course of carrying out the duties and obligations of the **information manager** under the agreement and under FIPPA.

'Unauthorized access' also occurs when others gain access to **personal information** in the custody or under the control of the **information manager** through improper, inadvertent or accidental disclosure or surreptitious means.

The information management agreement should:

- clearly set out the purposes for which **personal information** can be used by the **information manager** and its officers and employees – the 'authorized uses';

- state that only those officers and employees of the **information manager** who need to know the information to carry out their duties under the agreement are to have access to the **personal information**;

[300] Clause 87(i) of FIPPA.

[301] Subsection 44.1(3) of FIPPA.

- state that the officers and employees of the **information manager** will only have access to the minimum amount of **personal information** necessary to carry out their duties under the agreement; and

- include the security measures the **information manager** must put in place to prevent unauthorized access by officers, employees and others. Appropriate security measures will include physical, administrative and procedural, and technical measures.

(ii) Unauthorized use

'Unauthorized use' of **personal information** occurs where the information is used, dealt with or employed[302] for a purpose that is not permitted under the information management agreement.

The information management agreement should:

- clearly set out the purposes for which **personal information** can be used by the **information manager** and its officers and employees – the 'authorized uses';

  Remember: the **public body** can only authorize the **information manager** to use the **personal information** for the purpose of "processing, storing or destroying it or providing the **public body** with information management or information technology services".[303]

  Also remember: a **public body** cannot authorize its **information manager** to do anything that the **public body** itself cannot do. This means, for example, that a **public body** cannot authorize its **information manager** to use the **personal information** if the **public body** would not have authority to use it for that purpose under FIPPA.[304]

- state that the **information manager** is responsible for ensuring that **personal information** is used by its officers and employees only for these authorized purposes;

---

302 *Black's Law Dictionary, 6th Edition*.

303 Subsection 44.1(2) of FIPPA.

304 Subsection 44.1(2) of FIPPA.

- include the security measures the **information manager** must put in place to prevent unauthorized use of the **personal information** by its officers and employees. Appropriate security measures will include physical, administrative and procedural (e.g. policies, training, etc.) and technical measures.

(iii) Unauthorized disclosure

'Unauthorized disclosure' occurs when **personal information** is made known, revealed, exposed,[305] shown, provided, sold, given or shared by the **information manager** in circumstances not permitted under the agreement.

The information management agreement should:

- restrict disclosure by the **information manager** and its officers and employees of any **personal information** obtained in the course of carrying out the agreement. Disclosure of **personal information** by an **information manager** should be strictly limited to disclosures that a reasonable person would agree are necessary and appropriate in all the circumstances – e.g. where the disclosure is required by a law of Manitoba or Canada.

  Also remember: a **public body** cannot authorize its **information manager** to do anything that the **public body** itself cannot do. This means, for example, that a **public body** cannot authorize its **information manager** to disclose **personal information** if the **public body** would not have authority to disclose it under FIPPA.[306]

- include the security measures the **information manager** must put in place to prevent unauthorized disclosure of the **personal information** by its officers and employees. Appropriate security measures will include physical, administrative and procedural, and technical measures.

---

[305] *The Concise Oxford Dictionary, 9th Edition*; *Black's Law Dictionary, 6th Edition*.

[306] Subsection 44.1(2) of FIPPA.

(iv) Unauthorized destruction

'Unauthorized destruction' occurs when **personal information** is destroyed in a manner that does not comply with applicable legal or contractual requirements.

(v) Unauthorized alteration

'Unauthorized alteration' occurs when **personal information** is altered or changed in a manner that does not comply with applicable legal or contractual requirements.

The information management agreement should also include:

- a requirement that the **information manager** obtain undertakings of confidentiality from its officers and employees;
- a requirement that the **information manager** comply with any policies, procedures or directions provided by the **public body** respecting the protection of the **personal information**;
- a requirement that the **information manager** notify the **public body** immediately if the **information manager** becomes aware of any unauthorized access to or use, disclosure, destruction or alteration of the **personal information**, or of any other breach of a term or condition of the agreement;
- provisions for monitoring the **information manager's** compliance with the obligations under the agreement and the **information manager's** obligations under FIPPA;
- provisions protecting **personal information** while it is being provided or transmitted to or from the **information manager**;
- provisions ensuring the **personal information** and all copies are returned to the **public body** in a secure manner, or are securely destroyed, when the agreement ends or is terminated;
- any other terms or conditions that are appropriate in the circumstances.

To ensure that the **public body's** privacy obligations under FIPPA are properly dealt with in an information management agreement, it is strongly recommended that **public bodies** consult with legal counsel.

DISCLOSURE FOR RESEARCH PURPOSES - [SECTION 47]

Disclosure for research purposes
47(1) A **public body** may disclose **personal information** for a research purpose only in accordance with this section.

Subsection 47(1) permits a **public body** to disclose **personal information** (that is, recorded information about identifiable individuals) for a research purpose only if the requirements of subsection 47(4) are met. Amongst other things, a written agreement protecting the **personal information** is required.

Disclosure for a research purpose under section 47 can include disclosure to another **public body** or to another person, corporation, etc.

Under section 47, a **public body** "may" disclose **personal information** for research purposes. The use of the word "may" indicates that the **public body** has a discretion to disclose the **personal information** for a research purpose. Section 47 authorizes or permits disclosure; it does not require disclosure.

The decision to disclose **personal information** for a research purpose under section 47 is made by the **head** of the **public body**, his or her delegate under section 81 of FIPPA or (in the case of a **minister**) his or her deputy.[307]

In determining whether to disclose **personal information** for research purposes, the **head** must, in addition to ensuring all the requirements in subsection 47(4) are met, determine whether or not to exercise his or her discretion to disclose the **personal information**, even though there is authority to do so. In exercising this discretion, the **head** must consider whether it is appropriate to disclose the information in the circumstances, taking into account both the potential harm that could result from disclosure (including the harm to an individual's privacy) and the consequences of withholding the information.

[307] *The Interpretation Act* of Manitoba, clause 31(1)(d). *The Interpretation* Act, C.C.S.M. c. I80 can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/i080e.php.

If a researcher requests access to statistical or anonymized information that does not, alone or in combination with information otherwise available, allow any individual or individuals to be identified, section 47 and Part 3 of FIPPA do not apply.
A request for **personal health information** by a researcher carrying out a health research project must be dealt with under section 24 of *The Personal Health Information Act*, and not under FIPPA.[308]

[308] *The Personal Health Information Act*, C.C.S.M. c. 33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

■ Conditions the Research Must Meet - [Clause 47(4)(b)]

Conditions of disclosure
47(4) The **head** of the **public body** may disclose **personal information** for a research purpose only if

(b) the **head** is satisfied that

(i) the **personal information** is requested for a *bona fide* research purpose,

(ii) the research purpose cannot reasonably be accomplished unless the **personal information** is provided in a form that identifies individuals,

(iii) it is unreasonable or impractical for the person proposing the research to obtain consent from the individuals the **personal information** is about, and

(iv) disclosure of the **personal information**, and any information linkage, is not likely to harm the individuals the information is about and the benefits to be derived from the research and any information linkage are clearly in the public interest;

Clause 47(4)(b) requires that the **head** of the **public body** must be satisfied that the research purpose meets four conditions before exercising his or her discretion to approve disclosure of **personal information** for a research purpose. Clauses 47(4)(c) and (d) set out additional conditions, respecting protection of **personal information** and the required research agreement, that must also be met.

The **head** must be satisfied that all of the following four conditions have been met by the proposed research project:

*(i) The **personal information** is requested for a bona fide research purpose. [paragraph 47(4)(b)(i)];*

"Research" means the systematic investigation into and study of materials, sources, etc. in order to establish facts and reach new conclusions, an endeavour to discover new or to collate old facts, etc. by scientific study or by a course of critical investigation.[309]

"Bona fide" means in or with good faith; honestly, openly and sincerely; without deceit or fraud; real, genuine and not feigned.[310]

Example:

If a research proposal has been approved and will be supervised by a research review committee established by a university to review the scientific and ethical value of research proposals and to oversee research projects, the research purpose would be *bona fide*.

*(ii) The research purpose cannot reasonably be accomplished unless the **personal information** is provided in a form that identifies individuals [paragraph 47(4)(b)(ii)].*

Personal information is provided in a "form that identifies individuals" if the information can be linked to a particular identifiable individual. For example:

- if an individual is named in the information or if the information contains other unique identifiers (such as an address, a Social Insurance Number, driver's licence number, etc.) the information is in a "form that identifies individuals";

309 Ontario Information and Privacy Commissioner Order P-666 (Re Ministry of Health, April 27, 1994). http://www.ipc.on.ca/images/Findings/Attached_PDF/P-666.pdf.

Also see Ontario Information and Privacy Commissioner Order P0-1741 (Re Ministry of the Solicitor General & Correctional Services, January 18, 2000) which accepted the definition of "research" in Order P-666.

310 *Black's Law Dictionary, 6th Edition*.

- if it is reasonable to expect that an individual or individuals could be identified from the content of the information or from combining the information with information that is otherwise available, even though unique identifiers have been removed, the information is also in a "form that identifies individuals".

Under paragraph 47(4)(b)(ii), the **head** of the **public body** must be satisfied that the research cannot reasonably be carried out using statistical or anonymous information that does not, either by itself or when combined with information otherwise available, permit individuals to be identified.

*(iii) It is unreasonable or impractical for the person proposing the research to obtain consent from the individuals the **personal information** is about [paragraph 47(4)(b)(iii)].*

"Unreasonable" means going beyond the limits of what is reasonable or equitable.[311] "Impractical" means not feasible, realistic, actually possible.[312]

*(iv) Disclosure of the **personal information**, and any information linkage, is not likely to harm the individuals the information is about and the benefits to be derived from the research and any information linkage are clearly in the public interest [paragraph 47(4)(b)(iv)].*

Information linkage is the systematic comparison of sets of information (usually information banks or data banks) to establish relationships among data for a variety of reasons, including research or administrative purposes. In the context of research, information linkage is a means of linking the right information to the right people in a representative group under study.

Paragraph 47(4)(b)(iv) involves a balancing of two competing interests: the ability to carry out research and individual privacy. The **head** of the **public body** must be satisfied of two things before exercising his or her discretion to disclose **personal information** for a research purpose:

311 *The Concise Oxford Dictionary, 9th Edition*.

312 *The Concise Oxford Dictionary, 9th Edition*.

(a) Disclosure of the **personal information**, and any information linkage, is not likely to harm the individuals the information is about;

"Harm" means hurt or damage.[313] A disclosure of **personal information**, and any information linkage, is likely to cause harm if it will have an adverse impact on, or cause damage to, the individual the information is about. For example, the disclosure and any information linkage must not result in damage to an individual's reputation; an unreasonable invasion of his or her privacy; or denial of a job, benefit or service that has been or would otherwise have been awarded to the individual; etc.

(b) The benefits to be derived from the research and any information linkage are clearly in the public interest;

The disclosure of **personal information** for a research purpose must be considered in terms of the benefits to be derived. Some significant advantage or good must come from the research and any information linkage.

"Clearly in the public interest" means that the benefits from the research and the information linkage must apply to a wide segment of the public, not just a few individuals or interests, and that these benefits must be unambiguous, easily understood, not confused or doubtful.[314] The public benefits must outweigh the invasion of privacy that occurs with disclosure of the **personal information** to the researcher.

313 *The Concise Oxford Dictionary, 9th Edition*.

314 *The Concise Oxford Dictionary, 9th Edition*.

■ Conditions Protecting Personal Information - [Clause 47(4)(c)]

Conditions of disclosure
47(4) The **head** of the **public body** may disclose **personal information** for a research purpose only if

(c) the **head** of the **public body** has approved conditions relating to

(i) the protection of the **personal information**, including use, security and confidentiality,

(ii) the removal or destruction of individual identifiers at the earliest reasonable time, and

(iii) the prohibition of any subsequent use or disclosure of the **personal information** in a form that identifies individuals without the express written authorization of the **public body**;

Clause 47(4)(c) states that disclosure of **personal information** for a research purpose may take place only if the **head** of the **public body** has approved the researcher's proposed procedures for handling and protecting **personal information**. Clause 47(4)(d) requires the researcher to enter into a detailed written research agreement with the **public body** that includes these approved procedures.

The **head** must approve conditions respecting all of the following:

*(i) Conditions respecting the protection of the **personal information**, including use, security and confidentiality [paragraph 47(4)(c)(i)].*

The **head** must approve the proposed use of the **personal information** by the researcher in the context of the proposed research. This requires a clear description of the proposed research project and a description of who, in addition to the researcher, is to have access to the information and for what purpose.

"Security" refers to the steps, physical, administrative and procedural and technical, to be taken by the researcher to protect or guard the **personal information** from risks such as unauthorized access, use or disclosure. "Confidentiality" means keeping **personal information** secret[315] or private[316] and safe from access, use or disclosure by persons or disclosure to persons who are not authorized to see or handle it under the conditions approved by the **head** of the **public body** and contained in the research agreement.

Unauthorized access to **personal information** occurs when employees of the researcher, research assistants, etc. have access to **personal information** that they do not need to see or handle in order to carry out the approved research purpose. Unauthorized access also occurs where others gain access to **personal information** in the custody or under the control of the researcher through improper, inadvertent or accidental disclosure or surreptitious means.

Unauthorized disclosure occurs when **personal information** is made known, revealed, exposed,[317] shown, provided, sold; shared or given by the researcher in circumstances not approved by the **head**.

Appropriate security will require appropriate physical, administrative and procedural, and technical measures – such as locked filing cabinets; secured areas; computer controls and access codes; restricted work areas; encryption or encoding of data ; confidentiality undertakings from research assistants, employees and others who will have access to the **personal information**; etc.

315 *The Dictionary of Canadian Law*.

316 *Black's Law Dictionary, 6th Edition*.

317 *The Concise Oxford Dictionary, 9th Edition*; *Black's Law Dictionary, 6th Edition*.

(ii) Conditions respecting the removal or destruction of individual identifiers at the earliest reasonable time [paragraph 47(4)(c)(ii)].

"Removal or destruction of individual identifiers" means that the researcher is required to de-identify and make the **personal information** anonymous by deleting or destroying (in a secure manner appropriate to the medium in which the information is stored) all information which could identify or could potentially identify an individual, or which could be linked to an identifiable individual. Individual identifiers include name, address, and other unique identifiers such as a Social Insurance Number, driver's licence number, etc. and any information from which (alone or in combination with information otherwise available) it is reasonably possible to determine the identity of an individual.

This removal or destruction is to be done at the "earliest reasonable time". This time will vary depending on the nature of the research project and the comparisons the researcher is making among different sets of data.

(iii) *Conditions prohibiting any subsequent use or disclosure of the **personal information** in a form that identifies individuals without the express written authorization of the **public body** [paragraph 47(4)(c)(iii)].*

"Prohibition of any subsequent use or disclosure" of the **personal information** means that the researcher cannot use or disclose the **personal information** for any purpose other than the specific, approved research purpose without first obtaining written authorization from the **public body**.

The prohibition extends to any other use or disclosure of **personal information** in a form that (alone or in combination with any information otherwise available) identifies the individual the information is about. This includes but is not limited to:

- using the information for another study or research project;
- using the information to solicit funds from the subjects of the research;
- using the information to sell products or services to the subjects of the research;
- selling the information;
- giving the information to another person or organization for any purpose, including for other research, fundraising, etc.

■ Written Research Agreement Required - [Clause 47(4)(d)]

Conditions of disclosure
47(4) The **head** of the **public body** may disclose **personal information** for a research purpose only if

(d) the person to whom the **personal information** is disclosed has entered into a written agreement to comply with the approved conditions.

Clause 47(4)(d) states that the researcher must enter into a detailed written research agreement with the **public body** that includes the procedures for handling and protecting **personal information** approved by the **head** of the **public body** under clause 47(4)(c).

The Lieutenant Governor in Council may, under clause 87(i) of FIPPA, make regulations about the written agreement required under clause 47(4)(d); but, at present there are no regulations about research agreements under FIPPA.

A research agreement should usually include the following:

- a clear and complete description of the nature and purpose of the research, and who will be carrying it out;
- a clear and detailed description of the **personal information** requested;
- the duration of the research;
- how the **personal information** will be disclosed to the researcher, and how it will be protected while being disclosed to the researcher;
- an undertaking from the researcher that the **personal information** will only be used for the research purpose as approved by the **head** and as described in the agreement;
- the names of any persons (employees, research assistants, etc.) who will have access to the **personal information**, and a requirement that the researcher obtain written undertakings of confidentiality with respect to the **personal information** from all such persons;

- an undertaking from the researcher to ensure that only those employees who need to know the **personal information** to carry out the approved research purpose will be permitted to have access to the information;

- details of the measures to be taken by the researcher to protect the confidentiality of the **personal information**, including the security measures to be taken to protect the **personal information** from access, use and disclosure not authorized under the agreement;

- an undertaking that the researcher and all persons with access to the **personal information** will comply with any policies and procedures given by the **public body** respecting the confidentiality or protection of the **personal information**;

- an undertaking that the researcher will remove or destroy individual identifiers in a secure manner at the earliest reasonable time (where appropriate);

- a prohibition respecting any other or subsequent use or disclosure of the **personal information** in a form that identifies or potentially identifies individuals without the express written authorization of the **public body** (for example, in reports, publications, etc.);

- any additional terms and conditions respecting use, disclosure and security measures that are appropriate in the circumstances. For example, should the researcher be prohibited from contacting individuals the **personal information** is about without prior written authority from the **public body**?

- an undertaking that the researcher must notify the **public body** immediately in writing if he or she becomes aware of any unauthorized access to or use or disclosure of the **personal information**, or of any other breach of a term or condition of the agreement;

- a provision stating that, if the researcher fails to meet the conditions of the agreement, the agreement may immediately be terminated by the **public body** and all **personal information** provided, including any copies and **personal information** incorporated into draft reports, etc., will be returned to the **public body** or destroyed by the researcher, in a secure manner, as directed by the **public body**; etc.

These guidelines are very general. It is strongly recommended that legal counsel be consulted for assistance in developing a research agreement that meets the requirements of subsection 47(4) of FIPPA and that properly protects **personal information**.

DISCLOSURE OF A RECORD OVER 100 YEARS OLD - [SECTION 48]

Disclosure of records more than 100 years old
48 The **head** of a **public body** or the archives of a **public body** may disclose **personal information** in a **record** that is more than 100 years old.

Section 48 recognizes that the sensitivity of **personal information** decreases over time and that disclosure is unlikely to result in an unreasonable invasion of any individual's privacy where the information is in a **record** that is more than 100 years old.

Note: section 48 does not apply to **personal health information**.[318]

Under section 48 of FIPPA, records of historical value containing **personal information** (such as the professional qualifications of teachers in the nineteenth century) may be disclosed by the Archives of Manitoba, the archives of a **public body** or by the **public body** itself for historical research and other similar purposes.

As with the other disclosure provisions in FIPPA, section 48 authorizes or permits, but does not require, disclosure of **personal information**. The **head** of the **public body** or the archives must weigh any potential invasion of privacy involved (for example, to living family members) when deciding whether or not to disclose **personal information** in a **record** that is over 100 years old.

Related provisions are:

- Clause 17(4)(h) – where a formal application for access to a **record** is made under Part 2 of FIPPA, the exception to disclosure protecting an individual's privacy in section 17 does not apply if the **personal information** is about an individual who has been dead for more than 10 years. But, section 17 may apply to protect the privacy interests of living family members referred to in, or affected by disclosure of, the requested **record**. Also, remember: the right of access to **records** under Part 2 of FIPPA does not apply to **personal health information**.

[318] Section 35 of FIPPA.

- Clause 44(1)(z) – a **public body** may disclose **personal information** to a relative of a deceased individual if the **head** of the **public body** reasonably believes that disclosure is not an unreasonable invasion of the deceased's privacy.[319]

- Clause 22(2)(d) of *The Personal Health Information Act* states that a trustee (including a **public body**) may disclose **personal health information** to a relative of a deceased individual if the trustee reasonably believes that disclosure is not an unreasonable invasion of the deceased's privacy. [320]

  Personal health information in a clinical record compiled in a psychiatric facility respecting a deceased individual should only be disclosed in accordance with *The Mental Health Act.*[321]

[319] Clause 44(1)(z) is discussed earlier in this Chapter, under *Disclosure of Personal Information*.

[320] *The Personal Health Information Act* is discussed in Chapter 2, under *Relationship of FIPPA to Other Legislation*. *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

[321] *The Mental Health Act*, C.C.S.M. c. M110, is discussed in Chapter 2, under *Relationship of FIPPA to Other Legislation*. It can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/m110e.php.

PRIVACY IMPACT ASSESSMENTS

■ What is a "Privacy Impact Assessment"?

One purpose of FIPPA is to "protect individuals against unauthorized use or disclosure of their **personal information** by **public bodies**".[322] Section 41 of FIPPA states:

> **Protection of personal information**
> **41** The **head** of a **public body** shall, in accordance with any requirements set out in the regulations, protect **personal information** by making reasonable security arrangements against such risks as unauthorized access, use, disclosure or destruction.

An aspect of this duty to protect **personal information**, is the duty to prevent, to the extent possible, breaches of information privacy before they occur. The "privacy impact assessment" process is one tool that can help accomplish this.

> 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.[323]

A privacy impact assessment involves much more than completing a form or a checklist. It is an assessment, risk identification and risk mitigation process that requires a variety of skills.

- The federal government's Privacy Impact Assessment Policy describes the process as a "shared management responsibility", a "cooperative endeavour" that requires a variety of skill sets including those of program managers, technical specialists and privacy and legal advisors.

---

322 Clause 2(d) of FIPPA, discussed in Chapter 1, under *Purposes of FIPPA*.

323 Excerpt from the Manitoba Ombudsman's Special Report, October 2003: *Respecting Privacy – A Compliance Review Tool for Manitoba's Information Privacy Laws.*

- It is not limited to 'assessing' compliance with legal requirements, although this is important. It also involves risk identification and mitigation.

- The privacy impact assessment process is based on the privacy principles common to all information privacy legislation, including FIPPA. These privacy principles are discussed earlier in this Chapter, under *The Privacy Principles in FIPPA*.

■ When Should a Privacy Impact Assessment be carried out?

Note: there may be a legal or policy requirement to carry out a privacy impact assessment (discussed below).

Generally, it is good practice to carry out a privacy impact assessment when a **public body**:

- is developing or modifying a program, practice, information system or legislation that involves **personal information**;

- is embarking on any other initiative or activity that involves **personal information**.[324]

The process can also be used to review existing services, programs and activities, to ensure that all privacy requirements continue to be met, identify new risks to privacy because of changes in technology, etc.

Note: under FIPPA and *The Personal Health Information Act*,[325] the **Ombudsman** has the power to carry out privacy audits and reviews of existing programs and activities, as well as new ones.[326]

---

[324] Excerpt from the Manitoba Ombudsman's Special Report, October 2003: *Respecting Privacy – A Compliance Review Tool for Manitoba's Information Privacy Laws.*

[325] *The Personal Health Information Act*, C.C.S.M. c. P33.5, can be found at: http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php.

[326] See Part 4 of FIPPA, discussed in Chapter 7 of this Manual.

■ Why Carry Out a Privacy Impact Assessment?

(a) It may be required by law or policy.

Currently, FIPPA does not require that a **public body** carry out a privacy impact assessment. But there are government policies that may require or recommend that one be done.

- The Information and Privacy Policy Secretariat of the Department of Sport, Culture and Heritage has developed a 'corporate' Privacy Impact Assessment process for use by government **departments** and **government agencies**. The process has been approved by the Service Transformation and Information Communication Technologies Executive Coordinating Committee of Deputy Ministers. Contact the Information and Privacy Policy Secretariat for more information about this process.

(b) It's a good way to determine if legal requirements respecting information privacy are being, or will be, met.

(c) Done properly, a privacy impact assessment identifies potential risks to privacy – so that measures to avoid, eliminate or reduce these risks can be identified and put in place in a timely and cost effective manner.

(d) It can assist managers in making informed decisions with respect to policy, system design and procurement.

(d) Building privacy into a service, program or activity at the outset saves time, effort and money.

(f) The process produces a 'living' document that can be updated to identify privacy requirements and identify and avoid or manage privacy risks at all stages of a program, service or activity.

(g) It is evidence that a **public body** respects privacy and is acting with 'due diligence' – to the **Ombudsman** and to the public.

(h) The **Ombudsman's** office will likely apply similar considerations when assessing compliance with the privacy protection requirements in FIPPA and when carrying out privacy audits under FIPPA.

(i) The process can be an effective tool for building public trust.

(j) And, there are risks associated with not conducting a privacy impact assessment:

- the risk to the privacy of individuals – once privacy is lost, little or nothing can be done to restore it;
- loss of public trust and confidence in the **public body's** or the government's commitment to privacy protection required by legislation – bringing the service, program or activity, the **public body** and the government into disrepute.
- services, programs or activities – and electronic systems in particular – may have to be reconsidered, redesigned or retrofitted, involving substantial cost and time;
- **personal information** may be disclosed or "shared" through information sharing agreements or practices that do not comply with FIPPA or "best practices";
- government and its **employees** may be exposed to liability.[327]

[327] Excerpt from the Manitoba Ombudsman's Special Report, October 2003: *Respecting Privacy – A Compliance Review Tool for Manitoba's Information Privacy Laws.*

■ Some Tips on How to Approach a Privacy Impact Assessment

1. Gather the right team of experts, specialists and advisors.

The privacy impact assessment process is an assessment, risk identification and risk mitigation process. To carry it out properly, a variety of skill sets will be needed – such as program managers, technical specialists and privacy and legal advisors.

The Information and Privacy Policy Secretariat of the Department of Tourism, Culture, Sport and Consumer Protection provides support to **departments** and **government agencies** through its Privacy Impact Assessment process. The Secretariat can:

- educate and inform staff of legislative requirements and best practices;
- assist with the preparation of documents;
- identify areas where risk mitigation is required;
- suggest suitable subject matter experts (such as legal counsel, security and information technology specialists and records managers).

It is strongly recommended that **departments** and **government agencies** contact the Secretariat for assistance early in the design stages.

2. At the outset, provide a detailed context.

This should include:

- a detailed overview of the proposed initiative;
- a description of the underlying purposes and rationale for the initiative and of the need for **personal information**;
- a detailed description of the information to be collected, used, etc.;
- a detailed description of the 'information flow' – who will use it and for what purposes; to whom will it be disclosed and for what purposes; etc. Don't forget use of the information by agents and contractors; planned disclosures; etc.;

- an analysis of how the proposed collection and handling of **personal information** balances the benefits of the proposed initiative and the impact on individual privacy. To determine if the impact on privacy is "reasonable and proportionate", the following three part test, which has been used by the **Ombudsman**, should be applied. Is the proposed initiative:

  (i) necessary to achieve the intended purpose;

  (ii) effective in achieving the intended purpose; and

  (iii) proportional – that is, the loss of privacy is proportional to the benefit gained and there is no less privacy intrusive means of achieving the purpose.[328]

3. Analyze, in detail, the 'information flow' using privacy principles – and the questions that flow from these principles – as the framework.

Each instance of collection, use, disclosure, retention, protection and disclosure of **personal information** must be 'tested' against the privacy principles that are reflected in FIPPA and *The Personal Health Information Act*. These principles are:

- Consent
- Accountability
- Identifying purposes (and informing of purposes)
- Limiting collection
- Limiting use, retention and disclosure
- Accuracy
- Security (safeguarding)
- Openness
- Access to and correcting one's own information
- Compliance (monitoring for and challenging compliance).[329]

[328] This three part test is discussed earlier in this Chapter, under *Preliminary Privacy Considerations – Necessary, Effective and Proportional*.

[329] These privacy principles are discussed earlier in this Chapter, under *The Privacy Principles of FIPPA*.

4. Use available tools as an aid, but don't be afraid to adjust them where necessary.

For example, adjustments to standard tools may be necessary if your **public body** handles both **personal information** and **personal health information**, or if legislation other than, or in addition to, FIPPA applies to information maintained by your **public body**.

Available tools include:

- The Information and Privacy Policy Secretariat's *Privacy Impact Assessment*. For further information, please contact the Secretariat at 204-945-1252.

- The Manitoba Ombudsman's *Privacy Impact Assessment* tool, accessible on their website at https://www.ombudsman.mb.ca/info/privacy-impact-assessment.html.