



**BORDER LAND SCHOOL DIVISION**

It's all about

**INFORMATION**

*...and*

**HOW WE DEAL WITH IT**

## Levels of SENSITIVITY of INFORMATION

A Rule of Thumb...

- Records of a general or common nature =  
**DISCREET INFORMATION**
- Records containing personal information =  
**PRIVILEGED INFORMATION**
- Records containing personal health information =  
**CONFIDENTIAL INFORMATION**
- Records relating to a Young Offender =  
**CLASSIFIED INFORMATIN**

The **Border Land School Division** expects all of its employees to be aware of legal requirements in regards to recorded INFORMATION.

In addition, it requires all to show good judgment, discretion, and respect for individuals in the way they deal with all types of INFORMATION at their disposal.

Information about students is PRIVILEGED and CONFIDENTIAL.

## TABLE OF CONTENTS

Preamble: It's All About INFORMATION

1. Purposes of This Pamphlet
2. Two Basic Human Rights
  - The right to **access** INFORMATION
  - The right to the **privacy** of INFORMATION
3. A Few Important Definitions
4. Overview of Significant Documents - Regarding INFORMATION
  - a) *The Freedom of Information and Protection of Privacy Act (FIPPA)* (2000)
  - b) Guidelines for the Retention/Disposition of School Division Records (2002)
  - c) Manitoba Pupil File Guidelines (2002)
  - d) Guide to Manitoba & *FIPPA* + Handbook for Educational Bodies (2000)
  - e) *The Personal Health Information Act (PHIA)* (2000)
  - f) *PHIA - A Brief or Summary for Public Bodies* (2001)
  - g) *Public Schools Act (PSA)* plus *Education Administration Act*.
  - h) *The Young Offenders Act (YOA)* (1984)
5. Requirements/Obligations Placed on School Divisions
6. Resulting Border Land School Division Measures
7. The Pledge of Confidentiality (PHIA)

## **Preamble**

The past 25 years or so have seen a tremendous increase in both the amount and ease of INFORMATION acquired, manipulated, and communicated by governments and other public bodies.

At the same time the need to recognize and protect the rights of the individual in regards to INFORMATION that governments and public bodies have in their possession has emerged, primarily through the passing of provincial legislation. Specific requirements result from it.

Forthcoming federal legislation will place similar obligations regarding INFORMATION on private organizations and businesses, effective **January 1, 2004** with the implementation of *The Personal Information Protection and Electronic Documents Act*.

### **1. PURPOSES OF THIS PAMPHLET**

The purposes of this pamphlet are as follows.

- (a) To provide you, as a member of the Border Land School Division, with basic and concise knowledge about recent legislation and related guidelines which deal with different aspects of INFORMATION.
- (b) To clearly identify the requirements placed on School Divisions as a result of the legislation.
- (c) To specify what the Border Land School Division is doing to satisfy those requirements.
- (d) To supply sufficient references to allow you to delve more deeply into the areas identified, if you so need or wish.
- (e) To provide you with sufficient orientation, as a prerequisite to your signing the Division's Pledge of Confidentiality, as mandated by *The Personal Health Information Act*.

## 2. TWO BASIC HUMAN RIGHTS

(a) There have been increasing demands on governments and local governments to be more accountable to their citizens, and to have better informed people, by making INFORMATION available. The **right to access** INFORMATION held by governments and public bodies, including INFORMATION about oneself, with some exceptions, is now recognized.

(b) There has concurrently developed an increasing insistence on the need to protect personal and personal health INFORMATION. The **right to privacy** for one's own INFORMATION held by our governments and public bodies is also now recognized.

The above rights may appear to be somewhat opposed notions-- the one providing access and the other protecting privacy by restricting access. The legislation, however, specifies what INFORMATION must, may, and may not be collected, used, maintained, and disclosed, and under what circumstances. It thereby attempts to respect both the access to, and the privacy of INFORMATION.

## 3. A FEW IMPORTANT DEFINITIONS

A basic understanding of the following terms is necessary to comprehend the recent INFORMATION legislation and guidelines.

### **Head**

The person(s) designated as Head of a public body, usually the Chair or the Whole Board. (*FIPPA, 80*)

### **Access and Privacy Officer**

The staff member of the public body (usually the Superintendent) to whom the Head delegates powers and duties. (*FIPPA, 81*)[*MR.64/98(1)*]

**Access and Privacy Coordinator**

The staff member of the public body (usually the Secretary-Treasurer) to whom responsibilities for the day-to-day administration of the Act (*FIPPA*) is given. [M.R. 64/98 (2)] This person is usually also responsible to **act as Records Manager/Security Officer**, in charge of developing and overseeing procedures for dealing with the public body records.

**Information Manager**

The person or group that processes, maintains, or destroys personal health information for a trustee. [PHIA, 1(1)]

**Trustee**

A health professional, health care facility, public body, or health services agency that collects or maintains personal health information. [PHIA,1(1)]

**Record**

It means a record of information in any form, that is retrievable, and includes information that is written, photographed, recorded, or stored in any manner, on any storage medium or by any means, including by graphic, electronic, or mechanical means. (*FIPPA*, 1)

**Personal Information**

It means recorded information about an identifiable individual, including: name, address, telephone number, e-mail address, age, sex, sexual orientation, ancestry, race, colour, nationality, ethnic origin, religion or creed, personal health information, blood type, fingerprints, hereditary characteristics, political beliefs, education, employment or occupation, educational history, source of income, financial circumstances, criminal history, personal views held, the views of others expressed about him/her, any identifying numbers or symbols, etc. (*FIPPA*, 1)

### **Personal Health Information**

It means recorded information about an identifiable individual that relates to: health, health care history, genetic information, provision of health care, payments for health care, PHIN number, other identifying health information. [PHIA 1(1)]

**A Public Body:** includes a local public body.

**A Local Public Body:** includes an educational body.

**An Educational Body:** includes a school division.

When those terms are used, they therefore include school divisions.

### **Third Party**

A person or group of persons or an organization other than:

- (a) the applicant who seeks to access information, and
- (b) the public body applied to.

## **4. OVERVIEW OF SIGNIFICANT DOCUMENTS THAT DEAL WITH INFORMATION**

### **(a) *Freedom of Information and Protection of Privacy Act (FIPPA) (2002)***

What *FIPPA* states

- Purposes of *FIPPA*: To allow any person a right of access to records in general, and to records containing personal information about himself or herself, in the custody or under the control of public bodies, and to request corrections to such records. *FIPPA* also intends to control that manner in which personal information is collected, used, or disclosed
- Applicants must apply on the prescribed form as per Regulation 64/98. There is a duty to assist. There are time limits.
- There are 4 mandatory exceptions to disclosure, where the Head (or delegate) must refuse disclosure. Example: it would constitute an unreasonable invasion of a third party's privacy. (Sections 17-20)

- There are 12 discretionary exceptions to disclosure, where disclosure may be refused. Example: disclosure may reasonably be expected to harm or threaten the security of any property or system. (Sections 21- 32)
- If Head (or delegate) thinks there might be an unreasonable invasion of the privacy of a third party, he/she will give notice to the third party, who can respond in writing. Head will decide on disclosure in 21 days (or less with third party response). Either the applicant or the third party may complain to the Ombudsman.
- Information about an individual may be collected if it is necessary. Only as much as needed should be collected, preferably directly from the individual. There are some exceptions, for example, where indirect collection is consented to, for the purpose of managing or administering personnel. When information is collected directly, the individual must be informed of the purpose, the legal authority to collect, and the name and telephone number of a person who can answer questions about the collection. (Disclaimer)
- A person can request a correction to information.
- Public bodies must have a policy regarding the retention of personal information.
- The use and disclosure of personal information is limited to the minimum amount necessary and only for employees who need to know, and for purposes (or related to) for which it was collected.
- The Ombudsman has powers and duties (investigate, report, etc.)
- Complaints about access or privacy may be made to the Ombudsman. The Ombudsman may initiate a complaint.
- An appeal to the courts may be made.
- Public bodies may charge set fees for providing information.
- There is protection from liability for acting in good faith.
- Typical offences: disclose in contravention; make a false statement to the Ombudsman; destroy or erase information to evade a request for access.  
Maximum penalty: \$50,000.00.
- Accompanying Regulation 64/98 deals with fees, forms for complaints, applications for access, etc.



### **(b) Guidelines for the Retention/Disposition of School Division Records (2002)**

This is a second edition of the Guidelines first issued in 1993. It reflects “important social, legislative, and technological changes which necessitated a review...” (p.1)

- The document ties responsibilities to the *PSA, FIPPA, PHIA, and YOA*. . It establishes retention periods for various records.
- It provides for the controlled destruction of records (if not archived).
- It emphasizes the need to have policies and procedures in place.

### **(c) Manitoba Pupil File Guidelines (2002)**

The Guidelines were issued “to assist school boards in carrying out their duties and responsibilities respecting student information.” (p.1)

- The document ties those responsibilities to *PSA, FIPPA, PHIA and YOA*. . It specifies what elements should be included in the school division’s written policies and procedures. (p.4.)
- It identifies the Principal’s responsibilities in this regard. (p.6)
- It defines the components of the pupil file (p. 10)
- It discusses access and privacy issues in specific relation to legislation.

### **(d) Guide to Manitoba’s *FIPPA* + Handbook for Educational Bodies (2000)**

The Guide reiterates in layman’s terms the information contained in *FIPPA*; thereby making it easier to understand.

- Relevant sections of the Act are referenced.
- The Handbook was designed to assist educational bodies to better understand and administer *FIPPA*. It is especially helpful by providing sample forms and letters for use in different access and disclosure situations.

**(e) *Personal Health Information Act (PHIA) (2000)***

*What PHIA states*

- Purposes of *PHIA*: To recognize the personal and sensitive nature of health information. To provide the right to access and request correction of one's personal health information maintained by a trustee. To control the collection, use, and disclosure of personal health information.
  - An individual has a right to examine and receive a copy of personal health information maintained by a trustee. Request is usually in writing. There is an obligation to assist and to respond quickly. The request may be transferred and applicant is to be so informed. The identity of the applicant is to be verified. A fee may be charged.
  - Access may be refused in some situations, for example, if access could endanger the health of the individual or others, or if it could identify a 3rd party who gave information in confidence.
  - Corrections can be requested by the individual.
  - Collection of information should be necessary, only as much as needed, and should be sought directly from the individual. There are some exceptions: if consent has been given, or time and circumstances do not allow direct collection.
  - When collected directly, the purpose of the collection, the name of the officer of the trustee who can answer questions about the collection must be provided.
- (Disclaimer)
- The trustee must have a written policy regarding the retention and destruction of personal health information.
  - Security safeguards are emphasized: administrative, physical, and technical.
  - Disclosure must be limited to the minimum amount necessary, to employees who need to know only, unless consent otherwise given, or a directly related purpose, or to prevent harm.

- Disclosure is possible without the individual's consent in some cases, for example to contact a relative in case of illness, or in accordance with usual medical practice, or for research purposes (with certain conditions).
- The powers and duties of the Ombudsman are similar to those outlined in *FIPPA*.
- Complaints about access and privacy are made to the Ombudsman.
- The rights of an individual may be exercised by another person, for example, a parent/guardian if the minor does not have the capacity to make health care decisions.
- No actions lie against a trustee or person who reasonably believed that use or disclosure was authorized under *PHIA*.
- Offences include: false statements, misleading the Ombudsman, obstructing an investigation destroying or erasing personal health information to evade requests for access.
- Fine: \$50,000.00/day on summary conviction.
- Accompanying Regulation 245/97 deals with obligations of trustees: a written policy and procedures for the security of information, including access restrictions, protection against hazards, safeguards for electronic form, orientation for employees, pledge of confidentiality, and an audit every two years.

**f) *PHIA* - A Brief Summary for Public Bodies (2001)**

Using the question-answer format, this document deals with *PHIA* information and references the appropriate sections of the Act. It deals with access, but especially emphasizes the protection of privacy obligations of trustees under the collection, use, disclosure, security, retention, and destruction of personal health information.

**(g) *Public Schools Act (PSA) + Education Administration Act***

The following sections of the *Public Schools Act* deal with aspects of personal and/or personal health information.

42.1 - Storage of information - pupil files.

42.2 - Definition of "pupil file".

42.3 - 42.6 - Access and disclosure issues

58.6 (c) - Access to pupil files - parents/guardians.

58.9 (2) (b) - Access to pupil file - pupil.

92.1 - Access to personnel records by a Teacher.

The *Education Administration Act*, under M.R. 468/88 deals with required procedures for pupil files.

**(h) *Youth Criminal Justice Act***

The *Youth Criminal Justice Act* has its own set of rules regarding information. Basically, it prohibits the publication of the identity of a Young Offender--and prevails over provincial legislation. For this reason, the Manitoba Pupil File Guidelines outline specific rules to follow regarding access to, retention, disclosure, and destruction of records relating to Young Offenders.

**5. REQUIREMENTS/OBLIGATIONS PLACED ON SCHOOL DIVISIONS**

The foregoing pieces of legislation and accompanying guidelines have placed several requirements or obligations on Manitoba school divisions. The major ones are as follows:

**(a) FIPPA**

- Contents of such policy are specified [40 (2)]
- Requirement to protect personal information. (41)
- Requirement to designate Head, Access and Privacy Officer, and Access Coordinator. (80, 81) [M.R. 64/98, 1,2]

**(b) PHIA (2000)**

- A requirement to establish a written policy concerning the retention and destruction of personal health information and to comply with that policy, in conformity with the regulations. [17(1) (2)]
- Ensure destruction of personal health information to protect privacy and keep a record of same. [17 (3) (4)]
- Obligation to protect personal health information by adopting reasonable administrative, technical, and physical safeguards that ensure the confidentiality, security, accuracy, and integrity of the information. [18 (1) (2), 19]
- Requirements for written security policies and procedures, access restrictions, safeguards for electronic information, authorized access for employees, orientation and training for employees, pledge of confidentiality, audit of security safeguards. [M.R.245/97 (2) - (8)]

**(c) PSA and Education Administration Act**

- Requirement to establish written procedures respecting pupil files (collection, storage, retrieval, use of information. (42.1, 42.2)
- Access to pupil files. (42.3 - 42.6) [58.6 (c)] [58.9(2) (b)]
- Requirement to make program information available. (58.2)  
[M.R. 468/88, 29 (1) (2)]
- Requirement to provide access to personnel files—Teachers. (92.1)
- Responsibility of Principal for pupil files. [M.R. 468/88, (28)]
- Requirement to keep a record of achievement of pupils, transcripts.  
[M.R. 468/88, (14) (15)]
- Responsibility to provide new school with pupil file, in the case of a transfer.  
[M.R. 468/88, 29 (3)]

**(d) Manitoba Pupil File Guidelines (2002)**

- Requirement to inform parents/guardians/students of purpose, content, and accessibility of the pupil file, at the time of enrolment. (p.3)
- Requirement for a policy specifying access by divisional personnel under the different pieces of legislation. (p.5)
- Requirement for policy respecting disclosure under the various pieces of legislation. (p. 5)
- Records Management policies to include responsibilities of Principals in cooperation with the Access and Privacy Coordinator. (p.6)
- Requirement to provide the following, when collecting information directly: purpose, legal authority to collect, name of person to answer questions. Disclaimer (p.8)
- Requirement to have policies concerning the retention and destruction of personal and personal health information. (p. 23)

**(e) Guidelines for the Retention and Disposition of School Division Records (2002)**

The guidelines reflect the requirements listed above, and so will not be repeated here. There is, however, one additional requirement to have a senior official of the School Division (usually the Secretary-Treasurer) act as Records Manager. (p. 7)

**(f) Youth Criminal Justice Act (YCJA)**

As mentioned earlier, Young Offender records are required to be dealt within accordance with *YCJA*, even if they are part of the pupil file or some other file. Access is very limited. Use is very restricted and disclosure is almost always prohibited.

## 6. RESULTING Border Land School Division MEASURES

In order to deal effectively with the obligations mandated by the Province of Manitoba in regards to INFORMATION, the **Border Land School Division** has, by resolution:

- designated the board of Trustees as the head;
- named the Superintendent of Schools as Access and Privacy Officer
- Appointed the Assistant Superintendent as Access and Privacy Coordinator, under *the Freedom of Information and Protection of Privacy Act*.

In addition, and in conformity with the requirements of the applicable legislation outlined above, the Board of Trustees has by resolution adopted the following policies and regulations:

- Record Management Policy
- Record Management Guideline
- Record Management Student files— Procedures
- Record Management Personnel Files—Guidelines
- Pledge of Confidentiality—Form

## 7. THE PLEDGE OF CONFIDENTIALITY

It is a regulatory requirement that you, as a member of **The Border Land School Division**, having received orientation and training dealing with the security of information policies and procedures of the Division, sign the Pledge of Confidentiality.

## PLEDGE OF CONFIDENTIALITY

As an employee of Border Land School Division, I acknowledge and understand that I may/will have access to personal health information (statutory definition below) about others, including students, the confidentiality and protection of which is governed by *The Personal Health Information Act*.

I further acknowledge and understand that the School Division has established written policies and procedures containing provisions for the security of personal health information in the Division's possession during its collection, use, disclosure, storage and destruction; provision for the recording of security breaches; and corrective procedures to address security breaches.

I further acknowledge that I have been provided orientation and that I have received or will receive on-going training about these policies and procedures.

I acknowledge that I am bound by the policies and procedures established by the School Division in accordance with the Act and I am aware that a consequence of breaching them is prosecution under the Act, and/or disciplinary action.

Signature: \_\_\_\_\_ Date Signed: \_\_\_\_\_

Print name: \_\_\_\_\_ Position: \_\_\_\_\_

### STATUTORY DEFINITION OF PERSONAL HEALTH INFORMATION

"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 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

"health care" means any care service or procedure

- (a) provided to diagnose treat or maintain an individual's physical or mental condition
- (b) provided to prevent disease or injury or promote health, or
- (c) the affects that 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.

"PHIN" means the personal health identification number assigned to an individual by the minister to uniquely identify the individual for health care purposes.