Administrative Procedure 2075

Records Management – Protection of Personal Health Information of Employees

Board Governance Policy Cross Reference: 1, 9, 13, 14, 15

Administrative Procedures Cross Reference:

Records Management

Records Retention and Disposition

Records Management – Protection of Personal Information of Students

Records Management - Protection of Personal Health Information of Students

Records Management - Protection of Information Under the *Youth Criminal Justice Act (Canada)*

Records Management - Protection of Personal Information of Employees

Records Management - Protection of Personal Health Information of Employees

Form Cross Reference:

Pledge of Confidentiality

Legal/Regulatory Reference:

Manitoba Education - Guidelines on the Retention and Disposition of School Division/ District Records

The Freedom of Information and Protection of Privacy Act

The Personal Health Information Act

The Public Schools Act

The Child and Family Services Act

Youth Criminal Justice Act (Canada)

Date Adopted: August 2006

Amended: May 2019

Introduction

The Brandon School Division (the "Division") is the custodian of Personal Health Information relating to its employees. The Division, as a public body, is responsible for protecting this information from unauthorized release or access. The Division recognizes the right of an individual to access information that the Division holds, including information about the individual, subject to certain specified exceptions and the right to privacy for Personal Health Information in the custody and control of public

bodies. This Administrative Procedure has been put into place to recognize those rights and to comply with the requirements of The Personal Health Information Act *(PHIA)* respecting the collection, use, disclosure, security, retention and destruction of Personal Health Information

Definitions

Annual Employee File means the content of the file as set out in that portion of this Administrative Procedure entitled "Annual Employee File".

Confidential Information means Personal Information and Personal Health Information and any other information collected by or about an individual which is not generally known to the public, including but not limited to information relating to a "young person" as defined by the Youth Criminal Justice Act (Canada) or which is deemed confidential by the Division.

FIPPA means The Freedom of Information and Protection of Privacy Act, C.C.S.M., c.F175 as amended from time to time.

Health means the condition of being sound in mind, body and spirit.

Health Care means any care, service or procedure

- provided to diagnose, treat or maintain an individual's health;
- provided to prevent disease or injury or promote health;
- 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.

Human Resources means the Human Resource Department of the Brandon School Division unless otherwise specified.

PHIA means The Personal Health Information Act, C.C.S.M., c.P33.5, as amended from time to time.

Personal Health Information means recorded information about an identifiable individual that relates to

- the individual's health, or health care history, including genetic information about the individual;
- the provision of health care to the individual;
- payment for health care provided to the individual; and includes
- the personal health identification number (PHIN) assigned to an individual by the minister of health to uniquely identify the individual for health care purposes, and any other identifying number, symbol or particular assigned to an individual; and

- 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.

Personal Information means recorded information about an identifiable individual, including

- the individual's name;
- the individual's home address, or home telephone, facsimile or e-mail number;
- information about the individual's age, gender, sexual orientation, marital or family status;
- information about the individual's ancestry, race, colour, nationality, or national or ethnic origin;
- information about the individual's religion or creed, or religious belief, association or activity;
- personal health information about the individual;
- the individual's blood type, fingerprints or other hereditary characteristics;
- information about the individual's political belief, association or activity;
- information about the individual's education, employment or occupation, or educational, employment or occupational history;
- information about the individual's source of income or financial circumstances, activities or history;
- information about the individual's criminal history, including regulatory offences;
- the individual's own personal views or opinions, except if they are about another person;
- the views or opinions expressed about the individual by another person; and
- an identifying number, symbol or other particular assigned to the individual.

Records Management Administrative Procedures means the Administrative Procedures of the Division relating to the collection, management, disclosure, protection, and destruction of records collected and maintained by the Division and shall include the following Administrative Procedures: 2090 -Records Management - Protection of Personal Information of Students; 2080 – Records Management - Protection of Personal Health Information of Students; 2070 – Records Management - Protection of Information under the Youth Criminal Justice Act (Canada); 2085 – Records Management - Protection of Personal Information of Employees; 2075 – Records Management - Protection of Personal Health Information of Employees, and 2095 - Records Retention and Disposition.

Senior Administration includes:

- the Superintendent/CEO of the Brandon School Division;
- the Assistant Superintendents of the Brandon School Division;
- the Secretary-Treasurer of the Brandon School Division; and
- the Assistant Secretary-Treasurer of the Brandon School Division.

Any terms not defined herein but defined in The Public Schools Act shall for the purpose of this Administrative Procedure have ascribed thereto the meanings set out in The Public Schools Act.

School Division Records Management

Responsibility for Records Management

The records manager of personal information of employees for the Division shall be the Director of Human Resources and the privacy officer for the Division will be the Secretary-Treasurer or designate, each of whom shall be responsible to administer their duties under this Administrative Procedure and who may delegate duties to each School Leader, site manager, department head or other person as they consider to be necessary.

Ownership of Records

All files are the property of the Division. Staff leaving employment of the Brandon School Division shall ensure that employee files and records in their possession are transferred to the appropriate member of the work site's administration who shall ensure that the files and materials are governed by the "File Control Procedure" set out in this procedure.

Notice

The following notice is to be included on all application forms, referral forms, reports, or any form where Personal Information or Personal Health Information is being collected in relation to an employee:

This Personal Information or Personal Health Information is being collected under the authority given to the Division under The Public Schools Act and will be used for educational purposes or to ensure the health and safety of students. The information is protected by the Protection of Privacy provisions of the The Freedom of Information and Protection of Privacy Act (including but not limited to section 37) and the Personal Health Information Act (including but not limited to Part 3, Division 1). If you have any questions about the collection, contact the Brandon School Division Access and Privacy Officer at (204) 729-3100 or by mail at the Brandon School Division, 1031 – 6th Street, Brandon, Manitoba, R7A 4K5.

Managing Employee Files

General

Each employee shall have a personnel file that will be organized and separated into two components: the Employment Information File and Health Information File. Both are considered part of the personnel file for definition, collection, use, disclosure, security, access, retention, destruction or transfer considerations. Information comprising the personnel file of an employee may be held in more than one location if a system of cross-reference is in place.

Employment Information File

An Employment Information File exists for all employees and shall contain:

- pre-employment materials, including but not limited to correspondence associated with the application for employment, curriculum vitae, transcripts, letters of reference and placement documents;
- information that the Division has for all employees such as birthdate, address, phone number, gender, etc.;
- information relating to the Employee's specific employment which includes, but is not limited to, employment start date, employment assignments, evaluations, signed and dated notes and other similar materials;
- copies of letters relating to Board actions respecting the employee, including initial appointment, sabbatical leaves, leaves of absence, administrative appointments, etc.;
- correspondence between the employee and the Division Office;
- materials respecting professional development and performance evaluation;
- materials used for payroll purposes;
- communications between external agencies and the Division as they relate to the Employee; and
- indication of whether there exists a Health Information File.

Whenever possible, there shall be no Personal Health Information contained in the Employment Information File portion of the Personnel File. However, from time to time it may be necessary for payroll and employment history reasons to have a record on file explaining a leave of absence or suspension. In those cases the Personal Health Information shall be disclosed only to the extent that it is reasonably necessary, with specific health information being severed from the record, with a fully intact record being stored in the Health Information File.

Health Information File

A Health Information File exists for some employees and shall contain:

- ongoing health/psycho-social/counseling information;
- correspondence to and from the Employee's physician; and
- all other Personal Health Information.

Any Personal Health Information contained in the Health Information File is to be governed by the provisions of The Personal Health Information Act.

The Personnel File is to be maintained by the records manager and all internal requests for access to the Personnel File shall be forwarded to the records manager who may designate duties as they see fit. Although the Personal Health Information File shall remain in the Personnel File for the purpose of storing information the records manager or designate shall ensure that the Personal Health Information File is not disclosed except where appropriate.

Access and Privacy

Access to Personnel Records under The Public Schools Act

A school board or a person acting on behalf of a school board shall

- provide a teacher with access to the teacher's personnel record upon request; and
- upon request by a teacher, attach to the personnel record the teacher's written objection to, or explanation or interpretation of, any matter contained in the personnel record.

Access to Personal Information under The Freedom of Information and Protection of Privacy Act (FIPPA)

The provisions of FIPPA are in addition to and do not replace existing procedures for access to records or information normally available to the public and thus do not replace the access provisions under The Public Schools Act.

Access to Personal Health Information under The Personal Health Information Act (PHIA)

An individual has a right, on request, to examine and receive a copy of their Personal Health Information maintained by the Division, subject to the exceptions set out in PHIA or any similar legislation, as amended from time to time. The Privacy Officer for the purpose of PHIA shall be the Secretary-Treasurer or designate.

Access to Records under other Legislative Authority

The Division shall provide access to records to any person where there is express legislative authority to do so.

Informal Access to Records

Nothing in this section shall preclude the Division from granting its employees access to their own Personnel Record without the need for a formal request for access. However, the Personnel File of an employee is the property of the Brandon School Division and as such the Division retains the right to refuse access if permitted by law.

Staff Access to Records

Staff access to files pertaining to other employees is only permitted to the extent that the information is necessary to assist the staff member in completing their employment duties. Where it is unclear as to whether such access is necessary, the School Leader shall make the determination at a school level, with or without input from the records manager, and the records manager will make the determination at the Divisional level. Staff shall only be granted access to the Personal Health Information File if approved by the Senior Administration of the Division or the records manager.

Third Party Requests for Information

Third party requests for Personal Health Information may only be granted where authorized under Part 2 of PHIA, as may be amended from time to time, or with written consent of the employee. Third party requests for information must be directed to the Privacy Officer who may delegate duties as they see fit.

Administrative Security

Human Resources shall ensure that each new employee is provided access to a copy of the Division's Record Management Administrative Procedures, and must be made familiar with the procedure therein by way of an orientation session. Every employee of the Division must receive ongoing training about these procedures. As required by relevant legislation, the Division must ensure that each new employee signs a pledge of confidentiality (see Form Pledge of Confidentiality). Before this pledge is executed, the employee must be provided access to a copy of the Division's Administrative Procedures entitled "Records Management –Protection of Personal Information of Students", "Records Management – Protection of Personal Health Information of Students", "Records Management – Protection of Information Under the *Youth Criminal Justice Act* (Canada)", "Records Management – Protection of Personal Information of Employees", and/or "Records Management – Protection of Personal Health Information of Employees", as may be appropriate, and must be made familiar with the procedures therein by way of

an orientation session. Every employee of the Division shall receive ongoing training about these procedures as required by the relevant legislation.

Use and Disclosure of Records

General

Personal health information shall only be used for the purpose for which it was collected. Personal health information shall only be disclosed in accordance with the laws of Canada and Manitoba, which include, but are not limited to, the provisions for disclosure under The Public Schools Act, The Child and Family Services Act, and The Personal Health Information Act, which are available to employees and students of the Division online free of charge on the Government of Manitoba's website. In addition, copies of The Personal Health Information Act are available in paper form at every school, work site and the Division office.

Consequences of Breaching PHIA

Every employee of the Division is bound by the procedures established by the Division in accordance with the provisions of PHIA relating to the access, use and disclosure of Personal Health Information. Consequences of breaching the procedures may include disciplinary action up to and including dismissal.

Every employee, trustee or information manager who commits an offense under Part 6 of PHIA may be prosecuted under that Act.

File Control Procedure

Retention and Destruction of Records

The Annual Employee File, which is subject to an annual review as set out above, at the expiration of the retention period set out in the Division's existing Administrative Procedure entitled "Records Retention and Disposition" and the existing guidelines established by Manitoba Education entitled "Guidelines on the Retention and Disposition of School Division/District Records", records will be destroyed under controlled confidential conditions unless deemed archival. These records are to be forwarded to the Division Office with a list or summary of contents to the records manager. The records manager will file the summaries or lists in a disposition of records log.

Disposition is either:

- destruction of records; or
- transfer of records to archives.

Files and records should be disposed of as soon as possible after the retention periods have lapsed. In most cases, this should be undertaken as an annual procedure.

The Division shall not destroy any record with the intent to evade a request for access under PHIA.

Where Personal Health Information is destroyed the following information must be recorded in a disposition of records log:

- the identity of the individual whose Personal Health Information is destroyed;
- the time period to which the information relates;
- the method of destruction; and
- the person responsible for supervising the destruction.

Archival Option

Permanent records should be moved into the archives designated in the Retention and Disposition Schedule. Archival options include:

- Provincial Archives of Manitoba – The Archives legislation enables the Division to transfer its permanent records to the Provincial Archives; and
- Divisional Archives – Divisional archives are established to ensure proper storage conditions and servicing of archival information. Each school will keep an up-to-date database of records stored in divisional archives.

Physical Security

The Division's administrative security officer will be the Secretary-Treasurer or designate, who may delegate to the School Leader, department head or site manager as they see fit, who shall ensure that a locked environment is established where all confidential information, including Personal Health Information, is stored or accessible. This could mean a whole wing, a room or a filing cabinet, or any combination thereof.

The administrative security officer must maintain a duplicate key for each office at the Brandon School Division head office and each School Leader or site manager must maintain a duplicate key for each office within their respective school or site.

Electronic doors, if applicable, must not be left open while the area is unattended and combinations must not be disclosed to unauthorized personnel.

Materials dealing with confidential information must be closed and not left open for viewing when away from desk or work area. Confidential information must be cleared from the desktop at the end of the day and placed in a secure location such as a locked filing cabinet. Portable computers must be secured in a locked area when not in use and sensitive data on the hard drive must be secured by password protection.

Employee Files are not to be removed from the work site by any staff member except for the purpose of transferring the record to the Division Office. The staff member transporting the files is responsible for ensuring an appropriate level of security and confidentiality at all times the file is in their possession. Records are not to be left unattended while being transported.

Notwithstanding the foregoing, any member of Senior Administration of the Division may remove the Personnel File of any employee from the Brandon School Division Office it if is being removed for the purpose of obtaining legal advice on the contents thereof. In that event, the member of Senior Administration transporting the files is responsible for ensuring an appropriate level of security and confidentiality at all times the file is in their possession. Records are not to be left unattended while being transported.

Notwithstanding the foregoing, in the event of an emergency where there is risk of the Personnel File being damaged or destroyed a staff person may remove the Personnel File from any school or office of the Brandon School Division where that risk exists provided they, as soon as practicable transport the file to another school or office of the Brandon School Division where it may be secured in accordance with this procedure.

Notwithstanding the foregoing, the Executive Secretary in the Substitute Booking Office of the Division may remove all or part of an employee's Employment Information File to facilitate booking substitute teachers for a school. The Executive Secretary in the Substitute Booking Office shall only use and/or remove that part of the file which is reasonably necessary for them to perform the duties of their employment. The Executive Secretary in the Substitute Booking Office is responsible for ensuring an appropriate level of security and confidentiality at all times the information is in their possession. Records are not to be left unattended while being transported and shall be maintained in a locked area, out of plain site when not in use.

Transmission of Confidential Information

Confidential information that is provided over the telephone may only be given if the identification of the requester is verified. This information must not be left on an answering machine or by voicemail.

Confidential information must be faxed only when required for urgent or emergent purposes and only sent under the following conditions:

- there is no reasonable possibility that the information being transmitted can be intercepted during transmission by unauthorized personnel;
- the individual sending the fax is authorized to release the information;
- the cover page of the fax indicates, where applicable, "Confidential information. Disclosure, distribution or copying of the content is strictly prohibited. If you have received this fax in error please notify the sender immediately."; and

Transmitting confidential information via e-mail must only be done if the venue of transmission is secure or the data is encrypted.

Electronic Security

The Division's electronic security officer will be the Secretary-Treasurer or designate who may delegate duties as they see fit. The Division's electronic security officer is responsible for ensuring that the following is adhered to:

- shared USERID and passwords must only be assigned where it is not feasible to assign an individual USERID because of degradation of service to the public. The electronic security officer must approve sharing of USERID's and passwords, a listing of which will be maintained;
- USERID or password must not be shared with anyone except as may be necessary for authorized personnel to perform maintenance on the Personal Computer in which case the password must be changed as soon as the maintenance is performed;
- the electronic security officer must delete an employee's USERID from the system as soon as possible after the termination of the individual's employment with the Division;
- USERID or password must not be taped to a computer or left where it is easily accessible;
- the electronic security officer or designate shall be responsible for maintaining a listing of such USERID's and passwords for the staff as may be reasonably necessary to maintain the computer system and network of the Division; and
- information must be encrypted; where feasible, when transporting electronic information on portable computers.

Employees shall be responsible for logging out of the computer system at the end of each workday. Employees must also log out or utilize password access when the computer will not be in use for a period exceeding ten (10) minutes.

Additional Safeguards for Electronic Health Information Systems

The Division's electronic security officer or designate shall ensure every electronic information system that the Division designs or acquires after December 11, 2000

- produces an electronic record of every successful or unsuccessful attempt to
  - gain access to the Personal Health Information maintained on the system,
  - add to, delete or modify the Personal Health Information maintained on the system; and
- records every transmission of Personal Health Information maintained on the system.

The Division's electronic security officer or designate shall regularly review the electronic records as produced above to document and detect any security breaches.

The requirements of this paragraph only apply to an electronic information system used by a trustee to maintain Personal Health Information.

Reporting Security Breaches

Any security breaches involving Personal Health Information are to be reported immediately

- to the School Leader if the breach occurs at school. The School Leader is then to inform the Divisional Privacy Officer using the Divisional "Incident Report" form, a copy of which is to be forwarded to the Assistant Superintendent; and
- to immediate supervisors if the breach is identified by a divisional employee. The immediate supervisor is then to inform the Privacy Officer in writing of the breach.

The Privacy Officer will investigate all security breaches and recommend corrective procedures and/or discipline measures, where appropriate, to address security breaches.

General

Reasonable precautions are to be taken to protect Personal Health Information from fire, theft, vandalism, deterioration, accidental destruction or loss and other hazards.

The Division shall conduct an audit of its security safeguards at least every two years and shall take steps to correct any deficiencies as soon as practicable.