



GUIDELINES FOR STUDENT HEALTH INFORMATION

Reconciling the *HIPA* and the *LAFOIP*



Issues

1. Applicable legislation
2. Student files
3. Consent and disclosure
4. E-mailing about students
5. Temporary and permanent cessations of practice
6. Retention
7. Security guidelines

Applicable Legislation

- Health Region employees are governed by the *Health Information Protection Act (HIPA)*.
- School Division employees are governed by the *Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP)*.
- *** Occupational therapists employed by a School Division are not subject to *HIPA* regulation, however, occupational therapists employed by the Health Region contracting in a school division are.

Are the statutes consistent?

- Yes!
- **Difference:**
 - *HIPA* – uses the term ‘trustee’ – the Health Region owns student health information and is trustee of the information in its possession.
 - Information is referred to as PHI.
 - *LAFOIP* – no use of ‘trustee’ – the School Division owns all student information gathered to aid in student learning.
 - Information is called ‘personal information’.
- A School Board and its employees are NOT trustees.

Applicable Legislation – Summary

- Health Region Employees – *HIPA*
 - Health Region and Occupational Therapist are ‘trustees’ of the student’s personal health information in OT’s possession
- School Division Employees – *LAFOIP*
 - School Division and Occupational Therapist are NOT trustees of the information.
 - Information is referred to as ‘personal information’ as defined in *LAFOIP*.
 - School Division is sole owner of personal information.

Student Files - General

- All student information collected on behalf of a School Division or disclosed to a School Division is retained in the student's cumulative file.
 - This includes the results of diagnostic tests and other assessments, as well as PHI.
- The information in the student's cumulative folder is owned by the School Division.

Student Files - *HIPA*

- Occupational therapist collects information in accordance with *HIPA* regulations (see Documentation Guidelines).
- Information is disclosed to School Division and retained by the school in the student's cumulative file.
- Occupational therapist retains their personal files in accordance with *HIPA* regulation and the documentation guidelines.

Student Files - *LAFOIP*

- Information collected by the occupational therapist is done on behalf of the School Division.
- This information will be stored in the student's cumulative file.
- The occupational therapist's personal files should be retained in accordance with School Board guidelines.
 - Physical/electronic file possession guidelines are virtually identical to the documentation guidelines.

Disclosure - General

- Disclosure of student health information (whether PHI under *HIPA* regulation or personal information under *LAFOIP* regulation) must be consistent with the purpose for gathering the information*.
- Purpose: to enhance student learning.
- *This is important when dealing with consent and is taken from section 5(2) and sections 26(1) and (2) and 27(2) and (3) of *HIPA* and sections 27 and 28 of *LAFOIP*.

Disclosure - *HIPA*

- Teachers and other educational staff are not trustees.
- Disclosure of PHI to a 'non-trustee' is explained in section 21 of *HIPA*: "The trustee must:"
 - a) Take reasonable steps to verify the identity of the person to whom the information is being disclosed;
 - b) Where disclosure is made without consent: take reasonable steps to ensure that the person receiving the information knows that the information is not to be used or disclosed for any purpose other than the purpose it was collected.

Consent – *HIPA*

1. Can be obtained expressly through a consent form signed by the student's parent or guardian; or
1. Can be obtained **without** express consent where disclosure is consistent with the purpose for gathering the information (section 27(2)).
 - This fact is true Health Region Employees (*HIPA*)
2. Must be informed, must be given voluntarily, and must not be obtained through misrepresentation, coercion, or fraud.

Disclosure - *LAFOIP*

- Same basic principle as *HIPA*: information should be disclosed for a purpose consistent with the purpose it was collected (*LAFOIP* section 27).
- No use of 'trustee': information is owned by School Division and may be disclosed to School Division employees for the purpose of enhancing that student's learning.
- May occur without consent where disclosure is consistent with the purpose for collection.

E-Mailing Student Information

- *HIPA*: E-mailing student records should be done in accordance with the documentation guidelines.
- *LAFOIP*: Guidelines suggested on Saskatchewan Schools Privacy Website are consistent with documentation guidelines.

E-Mail Confidentiality - Guidelines

- An OT transmitting records by e-mail should ensure that the confidentiality and security of the records are maintained during transmission.
 - Ensure the identity of the recipient of the e-mail;
 - State in the e-mail that it contains confidential information;
 - *Encrypt; or de-identify, and/or obtain consent for e-mail communication of records;
 - Storing e-mails on a mobile phone may create security issues.

De-Identifying E-Mails

- Not a necessary requirement
- Removing a student's name from an e-mail does not classify it as de-identified (section 2(d) of *HIPA*).
- Obtaining consent for e-mail communication is a viable alternative.

Summer Holidays - *HIPA*

- This would fall under the 'temporary cessation of practice' in the *HIPA*.
- The Health Region remains the trustee of the information throughout the cessation of practice.
- The School cannot be a trustee during summer holidays.

Summer Holidays - *HIPA*

- Health Region employees can follow the documentation guidelines by:
 - Creating a cessation plan;
 - Obtaining the consent of a designated trustee who can be the trustee during the cessation of practice;
 - Form A of the Documentation Guidelines contains a sample cessation plan.

Summer Holidays - *LAFOIP*

- The School Division owns and retains the student's cumulative file that contains the student information.
- Does not require a 'designated trustee'.

Termination of Position - *HIPA*

- Contract should explain what is to happen with the information if the contract is terminated.
- If files are to be turned over to the School Division, they will be retained by the School Division in accordance with the **School Board Privacy Commission** guidelines.
- If files are kept by occupational therapist, they should be retained in accordance with the documentation guidelines and *HIPA*.

Termination of Position - *LAFOIP*

- All information obtained by the occupational therapist is owned by the School Division.
- If the position is eliminated, the occupational therapist no longer has any right to retain the information.
- It will be retained by the School Division in accordance with the **School Board Privacy Commission** guidelines.

Retention

- *HIPA* requires that information be retained for three years after the conclusion of client treatment or three years after the client reaches the age of majority.
- The **School Board Privacy Commission** states that student information will be retained for three years after the date that the student turns 22.
 - Except in the rare case of a very mature student, this will be much longer than is required under *HIPA*.

Security – Physical Files

- Security of physical files is outlined in documentation guidelines. Files are to be kept:
 - In a safe dry place;
 - In a locked cabinet;
 - If transported in a car, they are not to be left unattended in an unlocked vehicle.

Security – Electronic Documentation

- External Security: the SSOT Documentation Guidelines and the School Board regulations are very similar.
 - Appropriate firewalls;
 - Password protocols for access to information;
 - Encryption;
 - System back-ups.

Security – Electronic Documentation

- Internal Security: the School Board Privacy Commission suggests internal security measures as well.
 - Appropriate-use policies;
 - Educate employees on appropriate use and consequences of non-compliance;
 - Monitor system for breaches;
 - Enforce consequences for breaches.

Security – Mobile Phone Use

- Receiving confidential e-mails on a mobile phone creates a potential security risk.
- “Best Practices: Mobile Device Security”:
 - Limitation of information stored on cell-phone;
 - Password protection;
 - Authentication of receiver of information.

The End

- Thanks!



- My e-mail: dba693@mail.usask.ca