Understanding Privacy and Access to Information in the Education Setting

Fred Carter

Senior Policy & Technology Advisor

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

Osgoode Professional Development

October 24 2021

Information and Privacy Commissioner of Ontario

- Commissioner **Patricia Kosseim**—appointed by Ontario Legislature (July 1, 2020)
- 5 year term
- The Commissioner reports to the Legislative Assembly of Ontario and is independent of the government of the day
- In 2021, the Commissioner appointed:
  - Eric Ward, Assistant Commissioner, Strategic Initiatives and External Relations
  - Warren Mar, Assistant Commissioner, Tribunal and Dispute Resolution Services

IPC's mandate

- *Freedom of Information and Protection of Privacy Act* (*FIPPA*)
  - covers 300 provincial institutions
- *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*)
  - covers 1,200 municipal organizations
- *Personal Health Information Protection Act* (*PHIPA*)
  - covers individuals and organizations involved in the delivery of health care services
- *Child, Youth and Family Services Act* (Part X) (*CYFSA*)
  - children's aid societies, child/youth service providers
- *Anti-Racism Act (ARA)*
  - oversight of the privacy protective rules

IPC's roles

- IPC Roles:
  - investigate privacy complaints related to personal information
  - resolve appeals when there is a refusal to grant access to information
  - ensure compliance with the acts
  - review privacy policies and information practices
  - conduct research on access and privacy issues and provide comment on proposed government legislation and programs
  - reach out and educate the public, media and other stakeholders about Ontario's access and privacy laws and current issues affecting access and privacy

Applicable Law

Applicable Law

- *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)
  - Applies to municipal government institutions—including school boards
    - Sets out rules for the collection, use, disclosure, retention, access to and correction of, personal information
    - Applies to personal information of any individual—students, parents, community members
    - Provides a right of access to general records held by government organizations
- *Education Act*
  - Main law applying to the operation of school boards
    - Sets out rules relating to collection, use, disclosure, retention, access to and correction of information contained in the Ontario Student Record
- Other laws
  - *Personal Health Information Protection Act; Child, Youth and Family Services Act, Immunization of School Pupils Act; Personal Information Protection and Electronic Documents Act*

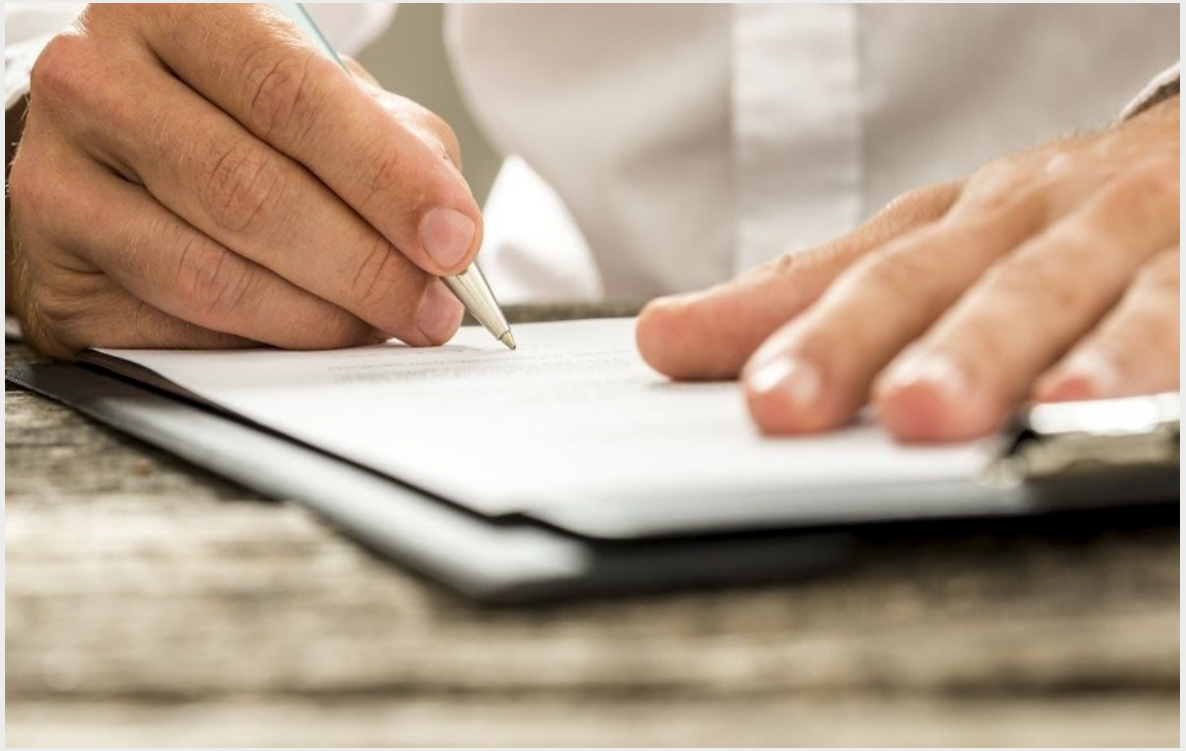
Principles of access

Ontario's access legislation sets out basic access principles:

- Information should be available to the public
- Exemptions from right of access should be limited and specific
- Disclosure should be reviewed independently

Requests under MFIPPA

- Three types of requests:
  - general information
  - personal information
  - correction
- In writing and a $5 fee
- 30 days



Right of appeal

A requester may appeal any decision:

- deny access
- charge fee, refuse to waive fee
- “deemed refusal”
- time extension
- deny a correction request

MFIPPA

- Personal Information=Recorded information about an identifiable individual, Eg.
  - name
  - Address
  - phone number
  - report cards
  - photos and videos
- Includes information in any format

Education Act—Ontario Student Record (OSR)

- Ongoing record of a student's progress through school
  - Must be established in accordance with Ministry of Education's "Ontario Student Record (OSR) Guideline, 2000" (the OSR Guideline)
  - Must contain specified information
- Other information collected by school boards does not form part of the OSR

Collection, Use and Disclosure of Personal Information

Collection of Personal Information

- School boards may only collect personal information if the collection is:
  - Expressly authorized by law
    - *Eg. Education Act* explicitly requires principals to collect information for inclusion in the OSR
  - Necessary for the proper administration of a lawfully authorized activity
    - Necessary means "more than merely helpful"—school boards must justify collection
- Consent is not a valid basis for collection of personal information

Notice of Collection

- School board must provide a notice of collection that informs the individual of:
  - The legal authority for the collection of their personal information
  - The purpose for which the personal information will be used
  - Contact information for a person who can answer questions about the collection

Use of Personal Information

- OSR may be used only for the information and use of supervisory officers, principals, teachers and early childhood educators of the school to improve the instruction and education of the student
- Under MFIPPA, school board may only use personal information:
  - For the purpose for which it was collected
  - For a purpose that is consistent with the purpose for which it was collected
    - A purpose is consistent if a person would reasonably expect that the information would be used that way
  - With consent
  - For a purpose for which the information may be disclosed to the school board under MFIPPA

Disclosure of Personal Information

- Supervisory officers, principals, teachers and early childhood educators may disclose personal information in the OSR to improve the instruction and education of the student
- Additional permitted disclosures include:
  - To the Ministry of Education or school board
  - Limited information to the medical officer of health

Cont'd

Disclosure of Personal Information

- Under MFIPPA, school boards may disclose personal information
  - For the purpose for which the information was collected
  - For a purpose that is consistent with the purpose for which it was collected
  - With consent
  - For the purpose of complying with law
  - In compelling circumstances affecting health or safety
  - To law enforcement in order to aid in an investigation

Cont'd

Disclosure of Personal Information

- School boards can disclose certain personal information in urgent situations
    - When compelling circumstances pose a threat to the health or safety of an individual
    - Where there is reasonable and probable grounds to believe that it is in the public interest and the record reveals a grave environmental, health or safety hazard to the public
  - Individual whose information is disclosed is notified
- School boards can disclose limited personal information when there is a need to notify a close relative, friend or spouse about an individual that is injured, ill or deceased, in order to facilitate contact

Cont'd

Disclosure of Personal Information

- There are some circumstances in which a school board is required to disclose personal information and may do so without consent
  - To medical officer of health
  - Notifying parents of harm to students
  - Disclosure to eligibility review officers (investigating eligibility for payments under Ontario Disability Support Program, Ontario Works, Family Benefits)
  - To report a child in need of protection to a children's aid society
  - Occupational health and safety

Specific Disclosures—To Children's Aid Society

- *Child, Youth and Family Services Act* requires any person that has reasonable grounds to suspect that a child under the age of 16 is in need of protection to immediately report it to a children's aid society
  - Prevails over any other act, including MFIPPA
  - Permits (but doesn't require) reporting for children 16 and 17 years of age
  - Gives legal protection to those reporting
- A person may also choose to provide information to a children's aid society review team who is investigating whether a child is in need of protection
  - The discretion to disclose in this circumstance prevails over any other act, including MFIPPA

Specific Disclosures—To Health Unit

- *Immunization of School Pupils Act* requires health units in Ontario to keep up-to-date immunization records for every student with respect to nine designated diseases
- The medical officer of health of the health unit can order the school to suspend a student whose immunization record is incomplete
- The medical officer of health of the health unit can require schools to disclose certain personal information about a student to the health unit in order to identify unvaccinated students

Specific Disclosures—To Law Enforcement

- MFIPPA permits school boards to disclose personal information to a law enforcement agency in Canada in certain circumstances
  - In response to a court order or subpoena
  - To aid a law enforcement investigation
    - After receiving request for the information from a law enforcement agency, if the request is
      - for specific information
      - made in the context of a specific law enforcement investigation
    - On the school board's own initiative if the board has reasonable basis to believe that a offence has occurred
  - In compelling circumstances affecting the health or safety of an individual

Specific Disclosures—School Photographs

- Collection of student photographs is considered necessary to the proper administration and operation of the school
- Disclosure of limited personal information to school photography company for the purpose of selling photos to families is permitted because it could be reasonably expected (See IPC privacy report MC16-4 and MC16-5)
- Notice and the opportunity to opt-out should be clearly given

Consent

Consent

- The rules around age of consent are different under *MFIPPA* and the *Education Act*
- Under *MFIPPA*
  - An individual with lawful custody of a child under 16 years of age may consent on the child's behalf
  - The child may also provide consent
  - Once the child turns 16 the parent or guardian may no longer consent on their behalf
- Under the *Education Act*
  - The parent or guardian of a student under 18 may provide written consent for the use or disclosure of information in the OSR

Safeguarding Personal Information

Safeguarding Personal Information

Cyber Security Awareness Month

- Define, document and put in place reasonable measures to protect records from inadvertent destruction or damage
- Take reasonable steps to prevent unauthorized access to their records, and ensure it is accessed only by those who need it to perform their duties
- Implement appropriate administrative, physical and technical measures to protect personal information

UPDATED OCTOBER 2022

TECHNOLOGY FACT SHEET

How to Protect Against Ransomware

Ransomware is a top threat facing Ontario organizations. Ransomware attacks can destroy vital records, knock out critical systems and services, and put sensitive information into the hands of criminals.

Organizations subject to Ontario's access and privacy laws must ensure that their cybersecurity programs include reasonable measures to protect their information holdings. This fact sheet is meant to be a useful overview for organizations and the people they serve.

This guide by the Office of the Information and Privacy Commissioner of Ontario (IPC) is for informational purposes only and should not be relied upon as a substitute for the legislation itself, or as legal advice. It is intended to enhance understanding of rights and obligations under Ontario's access and privacy laws. It does not bind the IPC's Tribunal that may be called upon to independently investigate and decide upon an individual complaint or appeal based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guide, visit www.ipc.on.ca.

WHAT IS RANSOMWARE?

Ransomware attacks involve the digital extortion of an organization. Attackers gain control of an organization's data holdings and often threaten to take damaging action unless they receive payment. Most ransomware attacks involve at least one of the following tactics:

- **Lock out.** Attackers gain control of business-critical systems, file repositories, and backups. They also use tools such as encryption to lock an organization out of its own information and systems, refusing to restore access until they receive payment.
- **Data theft.** Attackers gain access to large volumes of information, copy these records to a location they control, and threaten to publish them unless they receive payment.

The Canadian Centre for Cybersecurity reports having knowledge of 235 ransomware attacks that affected Canadian organizations in 2021. The actual number is thought to be much higher because of underreporting. For example, a 2022 TELUS survey of 463 Canadian businesses found that 83

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Examples of Administrative, Technical Safeguards

Administrative Safeguards	Technical Safeguards to Protect Electronic Data	Physical Safeguards
• privacy and security policies and procedures • privacy and security training • confidentiality agreements • privacy impact assessments	• strong authentication and access controls • logging, auditing and monitoring • strong passwords and encryption • maintaining up to date software by applying the latest security patches • firewalls, hardened servers, intrusion detection and prevention, anti-virus, anti-spam, and/or anti-spyware software • protection against malicious and mobile code • threat risk assessments	• controlled access to locations where personal information is stored • locked cabinets • access cards and keys • identification, screening and supervision of visitors

Privacy Breaches

- **Privacy breach** = personal information is collected, used, disclosed in ways not authorized by the acts
  - Deliberate
  - Accidental

- IPC may **investigate** privacy complaints, report publicly on them:
  - cease and destroy improper collections
  - make recommendations

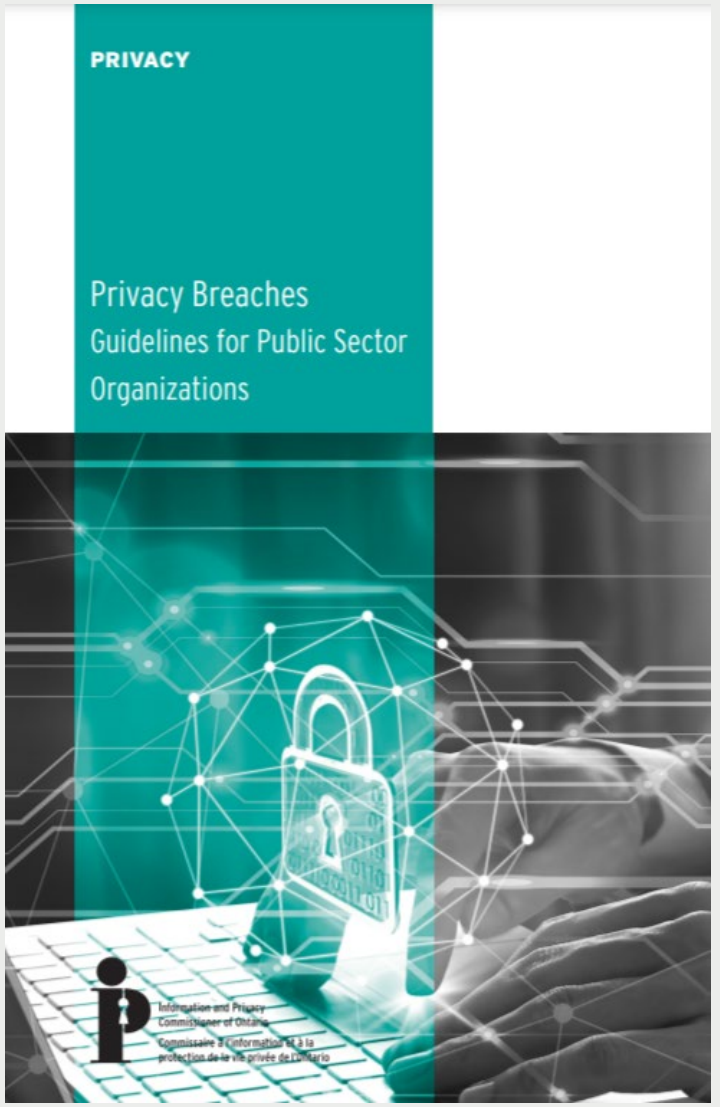
Responding to a Privacy Breach

STEP 1: Immediately Implement Privacy Breach Protocol

STEP 2: Stop and Contain the Breach

STEP 3: Notify Those Affected by the Breach

STEP 4: Investigation and Remediation



Accessing and Correcting Personal Information

Access to Personal Information

- Under MFIPPA
  - A child under 16 can access their own records
  - A parent or other person who has lawful custody of the child can also access records on the child's behalf until child is 16
  - Right of access is subject to some exceptions, Eg.
    - If it would be an unjustified invasion of another individual's privacy
    - If it could be expected to seriously threaten the safety or health of an individual
  - Must provide a copy of the record
- Under *Education Act*
  - Every student has the right to examine their OSR
  - Parents or guardians also have the right to examine the student's OSR until child is 18

Cont'd

Access to Personal Information

- Under *Education Act*
  - Request information directly from school
  - No cost
  - No timeline or appeal process
- Under MFIPPA
  - Formal request to school board directed to freedom of information coordinator
  - $5 fee
  - School board must respond within 30 days (with some exceptions for extension of time)
  - Additional fees may be charged—set out in the regulations; fee estimate required for amounts over $25

Accuracy and Correction of Personal Information

- School boards must take reasonable steps to ensure that personal information in their records is accurate and up to date
- The OSR Guideline requires the removal of material that is no longer "conducive to the improvement of the instruction of the student"

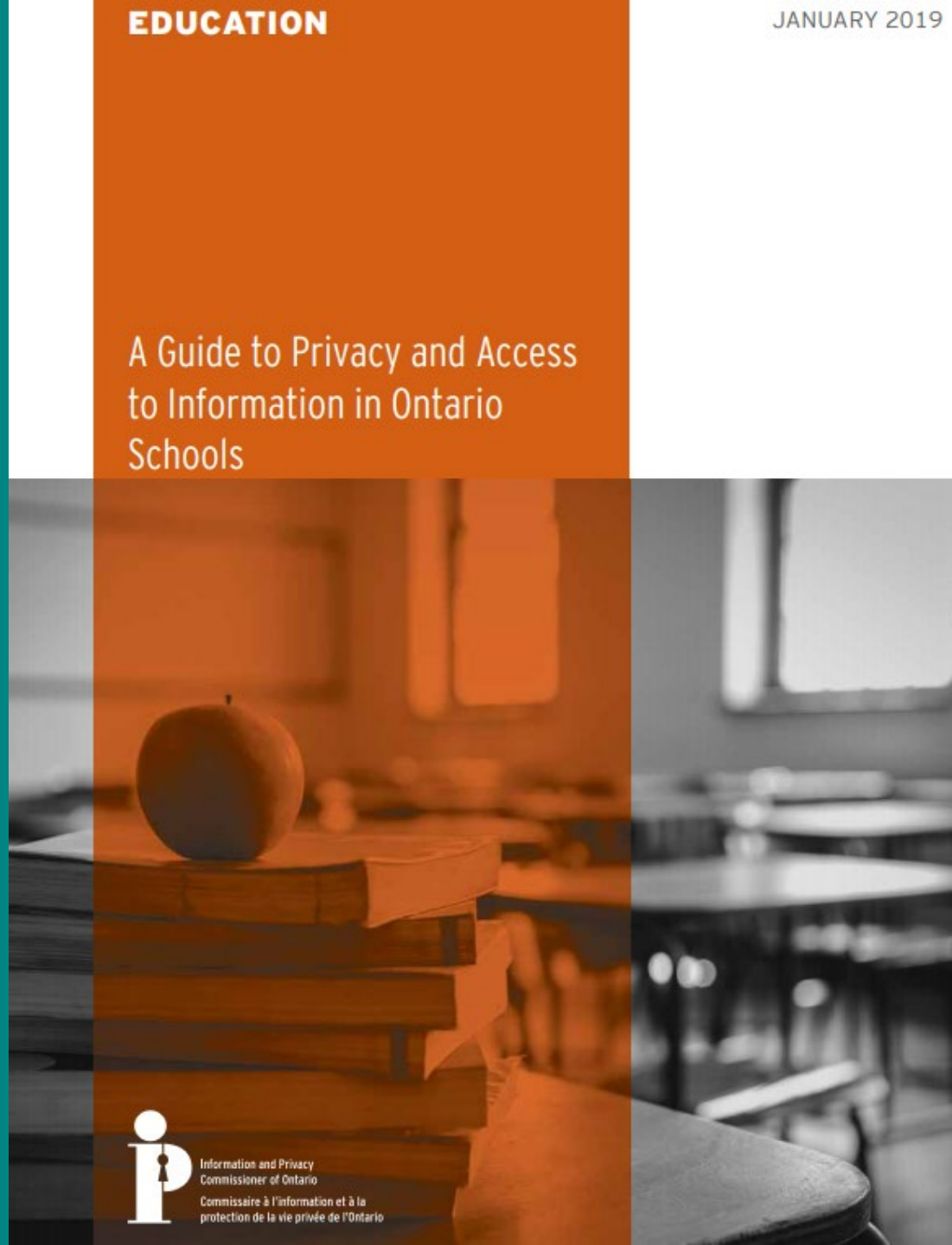
Cont'd

Accuracy and Correction of Personal Information

- If students or parents believe personal information in a record is inaccurate, they have a right to request correction of the information
- If a requested correction to the OSR is denied, the matter can be referred to a supervisory officer who can order the correction or a hearing
- If a request to correct information made under MFIPPA is denied, requester may have a statement of disagreement attached to the record and may appeal the decision to the IPC

IPC Guidance Documents

- A Guide to Privacy and Access to Information in Ontario Schools
- Privacy And Access to Information in Ontario Schools: A Guide for Educators (Fact Sheet)
- Privacy in the School (Fact Sheet)
- Protecting Your Students' Privacy Online (Fact Sheet)
- Your Child's Privacy in School (Fact Sheet)



Discussion

HOW TO CONTACT US

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965

Use of Online Educational Services

Use of Online Educational Services

- School boards are accountable for online educational services used in the classroom
- Online educational services used in the classroom must not improperly collect, use or disclose students' personal information
- Some online educational services:
  - Collect and retain personal information of students for their own non-educational purposes
  - Track and record students' online activities outside of the educational resource
  - Use students' behaviour and performance to target market products or services or disclose the information to third parties who will do so

Cont'd

Use of Online Educational Services

- Best Practices
  - Develop and implement policies to evaluate and support approved online educational services
  - Use only approved services
  - Provide privacy, security training and ongoing support to staff
  - Provide notice about personal information collected by online services and the purpose for the collection
  - Allow students and parents to opt-out
  - Set and enforce retention periods for accounts and different categories of personal information

IPC Privacy Complaint Reports

Use of cloud-based educational services by Ontario school boards:

1. MC18-48 – Security of attendance reporting platform (13 Apr 2021)
2. MC17-52 – Use of Google G-Suite for Education (23 Jul 2021)
3. MC18-17 – Use of third-party apps (7 Feb 2022)

Full text of these decisions available at:
www.ipc.on.ca/decisions

Holding Institutions Accountable

- IPC concluded three privacy complaint investigations involving Ontario school boards' use of online educational services.
- Each investigation differed in important ways, but all involved:
  - procurement and use of cloud-based services of third-party private-sector service providers acting as agents
  - direct access and use by students of online, account-based services
  - Parent concerns about improper collection, use and disclosure of students' personal information

Cont'd

Holding Institutions Accountable

- IPC investigators found school boards broadly in compliance with MFIPPA, but made recommendations to address some deficiencies, notably to:
  - improve transparency of information management practices, including enhanced notices of collection
  - establish clear privacy and security requirements, consistent with MFIPPA obligations, when contracting online educational services
  - ensure privacy and security requirements in contracts are kept up to date, and enforced

Cont'd

Extra Slides

Personal Health Information and School Boards

The *Personal Health Information Protection Act* (*PHIPA*)

- Applies to the collection, use and disclosure of personal health information by health information custodians, including when students receive health care in school
- Heath care includes any health-related observation, examination, assessment, care, service or procedure provided to students to:
  - diagnose, treat, or maintain their physical or mental wellbeing
  - prevent disease or injury
  - promote health
- Examples include:
  - providing care to a student who is not feeling well
  - providing psychological counselling
  - conducting an assessment—e.g. dental, vision, speech etc.

Health Information Custodians

- Most individuals and organization involved in the delivery of health care in Ontario are health information custodians, including:
  - health care practitioners
    - such as physicians, nurses, psychologists, speech-language pathologists, dental hygienists, optometrists, and social workers providing health care
  - a person who operates a group practice of health care practitioners
  - a community health or mental health centre, program or service whose primary purpose is the provision of health care

Health Information Custodians in Schools

Q: Who is the health information custodian when a health care practitioner provides health care to a student in school?

A: It depends on the way the relationship between the school and the health care practitioner is structured.

Cont'd

Health Information Custodians in Schools

1. A school may be the custodian if the school is:
   - operating a group practice of practitioners, or
   - operating a centre, program or service for community or mental health whose primary purpose is providing health care
2. A health care practitioner may be the custodian
   a) The custodian may be an individual health care practitioner who provides the service to the school; or
   b) The custodian may be a person who operates a group practice of practitioners who provide the services to the school

- If the custodian is the school or a person who operates a group practice, then individual health care practitioners would be "agents" to the custodian

Cont'd

Health Information Custodians in Schools

- Different arrangements are possible
- Employment contracts, service agreements, or other agreements should set out who is the custodian responsible for carrying out the duties and responsibilities required by *PHIPA*
- It should be clear to students and parents who the custodian is and a contact person must be identified

Cont'd

Health Information Custodians in Schools

- When determining who is the health information custodian, practitioners and schools should consider:
  - Who is in the best position to communicate with students and parents?
  - Who decides what information is to be collected and how it will be used and disclosed?
  - Where will records be maintained and who will ultimately be responsible for them?
  - What will happen when health care practitioners change positions?

Obligations on Health Information Custodians—Collection, Use and Disclosure

- Custodians may only collect, use or disclose a student's health information if:
  - they have consent from the student or parent* and it is necessary for a lawful purpose, or
  - it is permitted or required by *PHIPA*
- Custodians can only transfer student health records to a successor if the custodian makes reasonable efforts to give notice to the student or parent before transferring the records, or if this is not possible, as soon as is possible after the transfer

* Consider who is authorized to provide consent

Obligations on Health Information Custodians—Security

- Custodians must take **reasonable steps** to keep health information secure

Administrative	Technical	Physical
• privacy and security policies • auditing compliance with rules • privacy and security training • data minimization • confidentiality agreements • Privacy Impact Assessments	• strong authentication and access controls • detailed logging, auditing, monitoring • strong passwords, encryption • patch and change management • firewalls, anti-virus, anti-spam, anti-spyware • protection against malicious code • Threat Risk Assessments, ethical hacks	• controlled access to premises • controlled access to locations within premises where PI is stored • access cards and keys • ID, screening, supervision of visitors **NOTE** – when determining appropriate safeguards consider • sensitivity and amount of information • number and nature of people with access to the information • threats and risks associated with the information

Obligations on Health Information Custodians—Access and Correction

- Students have a right to access their health records that are held by a custodian
- Students also have the right to request correction of their health records if the record is inaccurate or incomplete

Obligations on Health Information Custodians—Transparency

- Custodians must designate a contact person responsible for:
  - Compliance with PHIPA
  - Responding to inquiries and complaints about the custodian's information practices
  - Responding to requests for access or correction of records
- A health information custodian must have a written public statement that describes:
  - The custodian's information practices
  - How to reach the contact person
  - How an individual may obtain access to or request correction of a record
  - How to make a complaint to the custodian and the IPC

Health Information Custodians Working for Non-Health Information Custodians

- Examples of Custodians Working for Non-Custodians
- Responsibilities of Custodians Disclosure of Personal Health Information by Custodians
- Health Information Records Kept In Other Places

Number 11
February 2006

Fact Sheet

Health Information Custodians Working for Non-Health Information Custodians

The *Personal Health Information Protection Act, 2004* (*PHIPA*) sets out rules for the collection, use and disclosure of personal health information by health information custodians (custodians).

While these rules are generally the same for all custodians, special considerations may apply in the case of custodians working for non-custodians.

What is a Health Information Custodian?

As defined in *PHIPA*, health information custodians include health care practitioners (see below), hospitals, psychiatric facilities, pharmacies, laboratories, nursing homes and long-term care facilities, homes for the aged and homes for special care, community care access corporations, ambulance services, boards of health, the Minister of Health and Long-Term Care and the Canadian Blood Services.

PHIPA defines a health care practitioner as: a person who is a member within the meaning of the *Regulated Health Professions Act, 1991* who provides health care; a person registered as a drugless practitioner under the *Drugless Practitioners Act* who provides health care; a person who is a member of the Ontario College of Social Workers and Social Service Workers who provides health care; and any other person whose primary function is to provide health care for payment. Examples of health care practitioners include: doctors, nurses, audiologists and speech-language pathologists, chiropractors, chiropodists, dental professionals, dieticians, medical radiation technologists, medical laboratory technologists, massage therapists, midwives, optometrists, occupational therapists, opticians, pharmacists, physiotherapists, psychologists and respiratory therapists.

PHIPA defines health care as any observation, examination, assessment, care, service or procedure that is done for a health-related purpose and that is carried out or provided:

- to diagnose, treat or maintain an individual's physical or mental condition;
- to prevent disease or injury or to promote health; or
- as part of palliative care.

Persons who do not provide health care are not health care practitioners.

Examples of Custodians Working for Non-Custodians

There are many examples of custodians working for non-custodians, including: