A Privacy Law Primer for Children’s Mental Health Professionals

Presentation to:
Children’s Mental Health Ontario – Annual Conference

November 26, 2018

Lonny J. Rosen C.S., Partner
@RosenSunshine
@LonnyRosen
Disclaimer

- Lonny Rosen is a lawyer in private practice and is a part-time member of the Consent and Capacity Board of Ontario.
- The comments expressed herein are made in Lonny Rosen’s personal capacity and not as a representative of the Consent and Capacity Board.
- This presentation is not legal advice!
Agenda

1. Introduction and Review of PHIPA Principles
2. Privacy Breaches and Reporting Obligations
3. Responsibilities to Safeguard PHI
4. Lessons from Recent PHIPA Decisions
Part 1: Introduction and Review of PHIPA Principles
Sources of Privacy and Confidentiality Obligations

• Legislation: PHIPA, PIPEDA, etc.
• IPC orders
• Civil cases
• Professional standards, codes of ethics, etc.
• College policies, discipline decisions, etc.
• Institutional policies, guidelines, code of ethics, etc.
PHIPA vs. PIPEDA

• The Personal Information Protection and Electronic Documents Act (PIPEDA) is federal legislation designed to regulate the collection, use and disclosure of personal information within the private sector.

• PIPEDA was not designed to address the intricacies of health information.

• The Personal Health Information Protection Act, 2004 (“PHIPA”) has been declared substantially similar to PIPEDA, and individuals covered by PHIPA are not also subject to PIPEDA with respect to health records.
Personal Health Information Protection Act, 2004 - PHIPA

• Applies to all health information custodians (HICs) and to individuals and organizations that receive information from HICs

• Regulates the way in which HICs collect, use, retain, transfer, disclose, provide access to and dispose of personal health information (PHI)

• Balances the right to privacy with the need to facilitate the effective provision of health care
Personal Health Information Protection Act, 2004 - PHIPA

• Ensures a right of access to an individual’s own PHI, subject to certain exceptions

• Provides a right to require corrections or amendments of an individual’s own PHI, subject to certain exceptions

• Sets out information practice requirements

• Provides remedies for privacy violations
What does PHIPA protect? Personal Health Information

• PHI includes any identifying information about an individual in oral or recorded form (i.e. paper and/or electronic records) that:
  • relates to the physical or mental health of an individual including their family health history
  • relates to providing health care, including identifying a person as a provider of health care to the individual
  • relates to payments or eligibility for health care or coverage for health care
  • is an individual’s health number
  • identifies an individual’s substitute decision-maker
What does PHIPA protect?
Personal Health Information

• Clients and patients do not have to be named for information to be considered PHI
• The test is whether the information identifies an individual or whether it is reasonably foreseeable in the circumstances that it could be used, either alone or with other information to identify the individual
To whom does PHIPA apply? - HICs

The following individuals or organizations who have custody or control of PHI:

• Health care practitioners
• Hospitals, IHFs, psychiatric facilities
• Pharmacies
• Laboratories
• Boards of health
• Community Care Access Centres
• Minister of Health and Long-Term Care
• A centre, program or service for community health or mental health whose primary purpose is the provision of health care
• ... and more
Agents of HICs

• Under PHIPA, HICs are permitted to employ agents to act for or on their behalf with respect to the collection, use and disclosure of PHI

• Agents = office staff such as receptionists, office managers, etc. because they act on behalf of the HIC with respect to PHI

• Agents have the same obligations with respect to PHI as the HICs for whom they work
Guiding Principles Under PHIPA

Identify Purposes

• Identify the purposes for which personal information is collected, use and disclosed at or before the time it is collected used or disclosed

Obtain Consent

• Consent is required for the collection, use or disclosure of personal information, subject to limited exceptions
Guiding Principles Under PHIPA

Limits

• The collection, use and disclosure of personal information should be limited to that which is necessary for the identified purposes, unless consent is obtained or otherwise required by law.

Accuracy

• Personal information should be as accurate, complete and up-to-date as necessary for the purposes for which it is to be used or disclosed.
Guiding Principles Under PHIPA

Safeguards

• Personal information must be protected by physical, technological and administrative security safeguards that are appropriate to the sensitivity of the personal information

Openness

• Individuals have the right to know about an organization’s policies and practices relating to the privacy and confidentiality
Guiding Principles Under PHIPA

Access and Correction

• Individuals have the right to access the information that is held about them upon request. They should be able to challenge the accuracy of the information and have it amended as appropriate.

Challenging Compliance

• Individuals should have an avenue for addressing a challenge/concern regarding the privacy or confidentiality of their personal information.
General Duties of HICs

- Establish information practices in accordance with PHIPA
- Designate a contact person to ensure the organization’s overall PHIPA compliance
- Notify individuals at the first reasonable opportunity when their PHI has been stolen, lost or accessed by unauthorized persons
- Ensure that all agents are appropriately informed of their duties under PHIPA
- Have a privacy statement that is made available to the public
A contact person is an agent of the HIC and is responsible for:

- Facilitating compliance with PHIPA
- Ensuring that all agents are appropriately informed of their duties under PHIPA
- Responding to inquiries about the HIC’s information practices
- Responding to requests for access to PHI and/or corrections to PHI
- Receiving complaints about alleged breaches of PHIPA
Privacy Policy / Statement

• HICs should have:
  • A Privacy Policy (may be internal); and
  • A Privacy Brochure or Poster (Statement of Information Practices)
Privacy Policy / Statement

• **Must set out:**
  • General description of the custodian’s information practice
  • What information is collected from and about client
  • The purposes for which PHI is collected
  • How PHI is protected
  • The requirement for consent and the client’s right to withhold or withdraw consent
  • How to contact the contact person
  • How an individual may obtain access to or request correction of a record of their PHI
  • How to make a complaint to the custodian and to the Privacy Commissioner
Consent

• Consent is required for the collection, use, disclosure of PHI

• Purposes of PHIPA include establishment of rules for the collection, use and disclosure of PHI that:
  • protect the confidentiality of the information,
  • protect the privacy of individuals with respect to that information, and at the same time,
  • facilitate the effective provision of health care. - s.1(a)

• Generally, need express or implied consent to collect, use or disclose PHI
Why Consent?

- Confidentiality is at the heart of health professional-patient or clinician-client relationship, and relationship of trust leads to better care.

- Where clients have opportunity to consent to collection, use or disclosure, they can be secure in belief that confidentiality will be maintained, enhancing the relationship of trust.
Exceptions to Consent Requirement

• Collection, use or disclosure of PHI in some circumstances does not require consent:
  • Where required or authorized by law (including where a search warrant, court order or summons/subpoena has been issued)
  • Where necessary, to prevent significant harm
What is Required for Valid Consent?

Consent must:

• be a consent of the individual (or the individual’s Substitute Decision Maker (SDM) if the individual is incapable)
• be knowledgeable
• relate to the information that is collected, used or disclosed
• not be obtained through deception or coercion - s.18(1)
Implied Consent (Assumed implied consent for health care)

PHIPA specifies several conditions when consent may be implied:

- Information exchanged between (disclosed to) custodians within the “circle of care” for the purpose of providing direct health care
- Using the name or address of person or SDM when PHI is collected, used or disclosed for fundraising purposes
- Disclosing the name and location of patient, to a religious organization, if the patient has previously provided information concerning affiliation
- A HIC may collect or use PHI for any purpose ancillary to provision of health care
Not defined under PHIPA

Describes health information custodians and their authorized agents

Does not include:

- Any health care provider who is not a part of the direct or follow-up team
- Evaluator under the Health Care Consent Act
- Assessor under the Substitute Decisions Act
- The Minister
- Any other person prescribed in the proposed Regulations
Express Consent

• Needed for:
  • Disclosure to a non-custodian outside the circle of care (eg. insurance provider)
  • Disclosure of information by one custodian to another custodian for a purpose outside of providing health care
  • Collection of information for marketing research
  • Collection of information (other than name and address) for fundraising purposes
Persons Who May Provide Consent

• A capable individual, regardless of age, can consent to collection, use, or disclosure of his or her own PHI

• Capacity is presumed

• Consent may be given on behalf of someone else:
  • if the individual is capable and 16 or over, anyone who is 16 or over whom the individual has authorized to act on his or her behalf may give or refuse consent on behalf of the individual
  • if the individual is less than 16 years of age, a parent of the child or youth may give consent on the child’s behalf, with some exceptions
  • if the individual is incapable of consenting, a person authorized to consent on behalf of the individual under this Act (i.e. the SDM) may give or refuse consent
  • if the individual is deceased, the deceased’s estate trustee or the person who has assumed responsibility for the administration of the estate may give or refuse consent
Persons Who May Provide Consent

• Where an individual can make a request, express an instruction or take a step, his or her SDM may make the request, express the instruction or take the step

• Where a HIC determines that a person is incapable of giving, refusing or withdrawing consent, that determination is reviewable by the Consent and Capacity Board

• An SDM can make decisions respecting collection, use or disclosure of PHI on behalf of the incapable person
Capacity to Give Consent

Capacity is:

• The ability to understand the information that is relevant to deciding whether to consent to the collection, use, or disclosure

and

• The ability to appreciate the reasonably foreseeable consequences of giving, not giving, or withholding or withdrawing consent
Ranking Order of SDMs

- PHIPA provides a hierarchy of SDMs who are authorized to consent on behalf of an incapable individual
- These SDMs are, in order of priority:
  - A statutory or court appointed guardian of the person or guardian of property (with authority)
  - attorney for personal care or attorney for property (with authority)
  - a representative appointed by the Consent and Capacity Board
  - the individual’s spouse or partner
  - individual’s child or parent (where “parent” is defined to include a child’s custodial parent, a children’s aid society or other legal guardian, but not a parent who has only a right of access)
  - a parent with only a right of access
  - a brother or sister
  - any other relative
  - Public Guardian and Trustee (as last resort)
Consent and Children

• If a child is capable, the child may consent
• If a child (young adult) is capable and 16 or older he or she is treated as an adult: he or she may authorize another capable person who is at least 16 years old to provide consent on his or her behalf, provided it is in writing
• If a child is capable and less than 16, a custodial parent, Children’s Aid Society or person lawfully entitled to stand in the place of a parent may consent EXCEPT:
  • If the PHI relates to treatment about which the child has made a decision on his or her own pursuant to Health Care Consent Act, 1996
  • If the PHI relates to counseling in which child participated on his or her own under the Child and Family Services Act
Consent and Children

• If a child is incapable, the same persons who may consent for an incapable individual can provide consent for an incapable child

• If a child is capable, even if less than 16, the child’s decision prevails over that of the parent or other SDM (where it conflicts)
PHIPA Principles Relating to Children

Best Practices

• To give effect to these rights, communicate to children/youth your practices, procedures, plans around PHI
• Document discussions, including questions asked to assess capacity and answers given
• Probe reason for decisions (in order to address consequences)
• Be sensitive to and avoid disputes
• Seek second opinion/supervision where assessment is controversial
Withdrawal of Consent

• An individual may withdraw consent by notifying the Custodian in writing
• A withdrawal does not have retroactive effect
The “lock box”

• The “lock box” allows a person to restrict the use that may be made of PHI, and to restrict who can see and use part or all of the person’s PHI that has been collected.

• But if disclosure is restricted, and the HIC is instructed to disclose some but not all of an individual’s PHI, if the HIC considers disclosure of the PHI in the “lock box”, the HIC must advise the other HIC (and possibly other providers of health care who access the PHI record) that it has not been authorized to disclose all information – s. 38(2)
Collection of Information

- Can only collect that information which is needed to meet purpose of collection
- Collection of PHI directly from individual requires consent, which will usually be implied by the fact that the individual is giving the information
- Information may be collected from third party if:
  - Client unable to provide
  - Question as to accuracy of the information that the individual provides
  - Obtaining consent would affect the timeliness of the care
Use of Information

• Consent is required for use of PHI, except where the use is:
  • for planning or delivering programs or services of the HIC
  • for the purpose of obtaining payment, processing, monitoring, verifying or reimbursing claims for payment
  • for risk management, for error management, in order to improve or maintain quality of services
  • for purpose for which it was collected or created and for all functions reasonably necessary (unless collected with consent or under s.36(1)(b) and individual expressly instructs otherwise)
  • for research (with research ethics board approval)
  • if permitted or required by law, subject to prescribed requirements and restrictions
Disclosure of Information

• Consent is required for disclosure of PHI, but there are a number of exceptions under PHIPA, including:

  • **Necessary for Care**: reasonably necessary for the provision of health care and it is not possible to get consent in a timely manner
  
  • **Eligibility**: determining or verifying eligibility for health care
  
  • **Risks**: where HIC believes on reasonable grounds that disclosure is necessary in order to eliminate or reduce a significant risk of serious bodily harm to a person or group
Disclosure of Information

• Consent is required for disclosure of PHI, but there are a number of exceptions under PHIPA, including:
  • **Proceedings:** for a variety of reasons relating to legal proceedings and in order to comply with summonses or court orders or procedural rules of production
  • **Legal Advice:** where an allegation, complaint or action is brought by a patient, the HIC can always review the patient’s PHI with a lawyer
  • **Permitted by law:** permitted or required by law, subject to prescribed requirements and restrictions
Access to PHI

• Every individual has right of access to his or her PHI, subject to exceptions
  • E.g. no right of access to raw data from standardized psychological tests or assessments
• Where an exception applies, individual has right of access to part of the record that can reasonably be severed
• After receiving a written request for access, a HIC responds within 30 days (subject to extension)
Exceptions to Right of Access to PHI

Access may be denied where information in the record was collected/created in connection with unconcluded inspection, investigation or legal proceeding or the record is subject to a legal privilege.

Access may also be denied where granting access could reasonably be expected to:

- lead to the identification of person who provided the information in confidence or was required to provide information;
- result in a risk of serious harm to treatment/recovery of the individual, or of serious bodily harm to the individual or others.
Handling Client Requests for Access to Records

• Determine what the client is requesting (i.e. entire record, specific entry, copy of lab report)
• Do not release the original record or leave the client alone with the original record
• Advise client if you intend to charge for the copy (such charges must be reasonable)
• Do not erase or modify any part of the record before providing it (can make additions, if done properly)
• If you are going to refuse, ensure rationale for refusal is reasonable and defensible (cannot refuse to avoid a legal proceeding) and advise client of right to make a complaint about the refusal to the IPC
Correction of a Record

• Upon request, correct the record where the individual demonstrates that the record is incomplete or inaccurate

• Not required to correct a professional opinion or observation made in good faith or a record that was not originally created by the HIC

• Where a HIC refuses to make a correction, must provide reasons for the refusal and inform the individual of his or her right to prepare a statement of disagreement and require that this be included in the record, and make a complaint to the IPC
Responsibilities to Safeguard PHI
Responsibilities of HICs to Safeguard PHI

• Under PHIPA, HICs must safeguard PHI in their custody or control by taking **steps that are reasonable in the circumstances** to ensure that:
  
  • PHI is protected against theft, loss and unauthorized use or disclosure
  
  • PHI records are protected against unauthorized copying, modification or disposal
  
  • PHI records are retained, transferred and disposed of in a secure manner
  
  • Safeguards can be physical, administrative, technological and cultural
Establishing a Culture of Privacy is also important and requires all staff and agents of the HIC:

- to be aware of HIC’s obligations
- to have concern for patients’ confidence in the HIC
- to realize the consequences of a breach or loss of PHI
- to focus on prevention of problems
- to take responsibility for ensuring that patients fully understand their rights and choices
Culture of Privacy

• With clients:
  • Establish ground rules at outset and stick to them (including for sharing PHI with family members, providers, etc.)
  • Address problematic areas with them (especially before sharing/releasing PHI)

• With Staff:
  • Do not engage in discussions about patients outside of clinical setting
  • Call colleagues on unsafe practices
Storage of PHI

- HICs must take reasonable steps to keep PHI securely stored
- What is reasonable varies depending on:
  - Sensitivity of the information and the risks to which it is exposed
  - The size of the organization
- Security measures must fit the HICs own circumstances, but should include:
  - physical safeguards
  - technological safeguards
  - administrative controls
Physical Safeguards

• locking filing cabinets storing PHI records
• ensuring that PHI records are supervised when they are not locked
• restricting office access to authorized personnel (i.e. through locks, pass codes and alarm systems)
• ensuring that faxes and printers are kept in a restricted area and are directly monitored while running
• protecting against the effects of fire
Storage of PHI

Technological Safeguards

• all staff should have their own computers, wherever possible, and at the very least, their own login IDs and passwords to access PHI
• passwords should not be easy to guess and should be changed regularly
• access should be removed as soon as a staff member leaves
• an administrator login and password
• automatic back-up for file recovery
• encryption, firewalls and virus scanners
• Audit trail
Storage of PHI

Administrative Controls

• a security protocol outlining the agencies rules regarding PHI security
• appointment of a staff member responsible for security
• staff training
• security clearances and access restrictions
• confidentiality agreements
• regular audits of actual practices to ensure compliance with the security protocol
Electronic Communication of PHI

• In communicating PHI, a HIC is obligated to ensure that unauthorized disclosure of PHI does not occur
• There are significant risks associated with the use of emerging forms of electronic communication, including vulnerability to interception and/or hacking
• As such, electronic communication should be avoided whenever possible and appropriate safeguards must be employed if it must be used
• Recommendation: Develop a policy!
Communication of PHI: by Fax

• Faxing should be limited to situations where no more secure practical alternative exists
• PHI should be de-identified to the greatest extent possible
• Fax machines should be located in a secure area
• Recipient should be contacted to confirm the fax number and that the recipient fax machine is in a secure area
• Always include cover letter including:
  • Name of sender and recipient
  • Warning that the information is intended for the named recipient only and to contact the sender if the communication is misdirected
• Recipient should be contacted to confirm receipt of fax
Communication of PHI: by Texting and E-mail

- Always potentially insecure
- Generally, should be discouraged
- Should only be used where:
  - Risks have been explained to client at the outset (and documented)
  - Consent has been obtained
- Texts and E-mails should not include any PHI
- Should be limited to communication about administrative matters (e.g. appointment scheduling)
Disposal of PHI

• Must take reasonable steps to ensure the secure disposal of PHI

• Reasonable steps include:
  • Written agreements with agents
  • Policy outlining disposal policies
  • Maintaining a ledger outlining the following particulars in the disposal process:
    • Identification of the PHI disposed of;
    • the manner in which PHI was disposed of;
    • the name of the individual to whom the PHI related;
    • the date of disposal; and
    • the name and telephone number of the individual who disposed of the PHI
Disposal – Paper Records

• For paper records, secure disposal consists of permanently destroying the documents by irreversible shredding (i.e. cross-cutting) or pulverizing, thus making them unreadable

• HIC is responsible for ensuring that steps are taken to ensure that no unauthorized person will have access to the records throughout the disposal process
Disposal – Electronic PHI

• Must also take steps to ensure secure disposal of electronic PHI - may involve physical destruction, deletion or overwriting the information

• See new Guidelines issued by IPC and/or consult an expert to ensure that electronic PHI is permanently destroyed
Retention of PHI

• No retention period established under PHIPA
• PHIPA requires that PHI records be kept for as long as needed to allow an individual to exhaust any legal recourse regarding a request for access
• HICs and their agents are required to refer to their governing legislation and professional standards
• Best practice is to retain PHI records for at least:
  • 10 years from time record was last updated; or
  • for minors, 10 years following 18th birthday.
Part 2: Privacy Breaches
Recent News Headlines

Privacy breach: Six GTA hospitals gave patient info to photographers
Mount Sinai, North York General, St. Joseph’s, Humber River, Toronto East General and Rouge Valley gave patient info to baby photographers.

Rouge Valley hospital privacy breach expands to affect 14,450 patients
Details on 14,450 patients at Ajax-Pickering site as well as Centenary were revealed to RESP company.

Hospital privacy violations rife in Ontario
More than 400 complaints about privacy breaches are lodged each year, yet only one prosecution has occurred since 2004.

Staffers snooped into 500 patients' files at Lakeridge Health
The Oshawa facility discovered a single breach of patient files last June; a subsequent review found 14 staffers had poked into more than 500 files.

Dentist’s patient information found scattered on Toronto street
Privacy Breaches

• Privacy breach = the loss, theft, or unauthorized collection, use or disclosure, of PHI or PI

• Under PHIPA, “use” means to view, handle or otherwise deal with PHI

• Important that organizations develop a Privacy Breach Management Protocol for addressing privacy breaches
Responding to a Health Privacy Breach: Guidelines for the Health Sector
Breach Management Protocol

Key Steps Recommended by the IPC:

STEP 1: NOTIFY STAFF AND OTHER CUSTODIANS

STEP 2: IDENTIFY THE SCOPE OF THE BREACH AND TAKE STEPS TO CONTAIN IT

STEP 3: NOTIFY THE INDIVIDUALS AFFECTED BY THE BREACH, THE IPC, AND/OR REGULATORY COLLEGES

STEP 4: INVESTIGATE AND REMEDIATE
Breach Management Protocol

STEP 1: NOTIFY STAFF AND OTHER CUSTODIANS

• Notify appropriate staff of the breach, including the privacy officer or other staff member responsible for privacy.

• Depending on the nature or seriousness of the privacy breach, contact senior management and technology and communications staff.

• If the breach involves PHI on an electronic system shared between multiple custodians, notify all affected custodians.
STEP 2: IDENTIFY THE SCOPE OF THE BREACH AND TAKE STEPS TO CONTAIN IT

• Identify the scope of the breach:
  • individuals or organizations involved or responsible
  • the nature and quantity of PHI that is affected.

• Retrieve any copies of PHI that have been disclosed.

• Ensure that no copies of PHI have been made or retained by anyone who was not authorized to receive the information.

• Record the person’s contact information in case follow-up is required.
STEP 2: IDENTIFY THE SCOPE OF THE BREACH AND TAKE STEPS TO CONTAIN IT (continued)

• Determine whether the breach would allow unauthorized access to any other PHI, for instance if it is on a shared system.

• Take whatever steps are appropriate, such as changing passwords and identification numbers and/or temporarily shutting down your computer system.

• In a case of unauthorized access by an agent, consider suspending their access rights
STEP 3: NOTIFY THE INDIVIDUALS AFFECTED BY THE BREACH, THE IPC, AND/OR THE REGULATORY COLLEGES

• PHIPA requires custodians to notify individuals affected by a breach at the first reasonable opportunity.

• Determine best form and timing of notification based on circumstances of the client and the breach.

• Consider whether there may be exceptional circumstances where direct notification is not possible or may be detrimental to the individual, and contact IPC or seek advice.
STEP 3: NOTIFY THE INDIVIDUALS AFFECTED BY THE BREACH, THE IPC, AND/OR THE REGULATORY COLLEGES (continued)

• When notifying individuals affected by a privacy breach, provide the following information:
  • where appropriate, the name of the agent responsible for the unauthorized access
  • the date of the breach
  • a description of the nature and scope of the breach
  • a description of the PHI that was subject to the breach
  • the measures implemented to contain the breach, and
  • the name and contact information of the person in your organization who can address inquiries
STEP 3: NOTIFY THE INDIVIDUALS AFFECTED BY THE BREACH, THE IPC, AND/OR THE REGULATORY COLLEGES (continued)

• Notice to affected individuals must include a statement letting them know they are entitled to make a complaint to the IPC.

• Address steps individuals should take if financial information or information from government-issued documents, such as health card numbers, are involved

• Note circumstances in which IPC or Regulatory Colleges must be notified (outlined below)
STEP 4: INVESTIGATE AND REMEDIATE

• Conduct an internal investigation to:
  • ensure the immediate requirements of containment and notification have been met
  • review the circumstances surrounding the breach, and
  • review the adequacy of existing policies and procedures in protecting PHI

• Review systems and consider changes to prevent breaches
STEP 4: INVESTIGATE AND REMEDIATE (continued)

- Keep a log of all privacy breaches and identify a person responsible for maintaining the log. For each privacy breach, record:
  - the name of the employee or agent that caused the breach, if relevant
  - the date of the breach
  - the nature, scope and cause of the breach
  - the number of individuals affected by the breach
  - a description of the PHI that was subject to the breach, and
  - a summary of the steps taken to respond to the breach.
The Information and Privacy Commissioner of Ontario ("IPC")

- The Information and Privacy Commissioner of Ontario (the "Commissioner") has been designated as the independent oversight body responsible for ensuring that HICs collect, use and disclose PHI in accordance with PHIPA
New Obligations on HICs in the Event of a Breach
Recent Amendments to PHIPA

- In the wake of a number of high-profile privacy breaches, the Ministry of Health and Long-Term Care introduced amendments to PHIPA through Bill 119
- Key Amendments include:
  - Doubling fines for offences under PHIPA from $50,000 to $100,000 for individuals and from $250,000 to $500,000 for organizations
  - Removal of limitation period for PHIPA prosecutions
  - Mandatory reporting of privacy breaches
New Obligations on Custodians in the Event of a Breach

• New obligations came into effect on October 1, 2017
• Where a custodian informs someone of a PHIPA breach, they must inform them that they are entitled to make a complaint to the IPC
• Intended to increase IPC oversight
• Obligation to notify the IPC of a breach where certain circumstances are met
• Obligation to provide annual report to the IPC on privacy breach statistics
When IPC Must be Notified

1. PHI was used or disclosed without authority by a person who knew or ought to have known that they were using or disclosing without authority
2. PHI was stolen;
3. After an initial loss or unauthorized use or disclosure of PHI, the PHI was or will be further used or disclosed without authority;
4. The loss or unauthorized use or disclosure of PHI is part of a pattern of similar losses or unauthorized uses or disclosures of PHI;
5. Unauthorized collection, use, disclosure, retention or disposal by an employee or agent of the Custodian (whether or not a member of a health College), and

- the employee is terminated, suspended or subjected to disciplinary action as a result of same, or
- the employee resigns and the Custodian has reasonable grounds to believe that the resignation is related to its investigation or other action with respect to same
When IPC Must be Notified

6. The Custodian determines that the privacy breach is **significant** using the following factors:
   - The sensitivity of the PHI
   - The volume of the PHI
   - Whether it involved many individuals’ PHI
   - Whether more than one employee or agent was responsible
   - Whether more than one Custodian or agent was responsible for the loss or unauthorized use or disclosure of the PHI
Where College Must be Notified

- HIC must notify College under the *Regulated Health Professions Act* where:
  - HIC terminates, suspends or takes other disciplinary actions against an employee who is a College member in relation to a privacy breach
  - Employee who is a member of a College resigns and HIC has reason to believe resignation relates to the employer’s investigation or other matter related to the privacy breach
Annual Reports to the IPC

• HICs are required to start tracking privacy breach statistics as of January 1, 2018 including theft, loss, unauthorized use and unauthorized disclosure of PHI

• Must provide the Commissioner with an annual report of the previous calendar year’s statistics, starting in March 2019
Privacy Breach Statistics

• Total number of thefts
• Identity of the thief
  • Employee
  • Stranger
  • Hacker/Ransomware
• Storage of PHI
  • Paper records
  • Electronic system
  • Portable electronic device (USB/laptop)
• Total number of individuals affected
Lost PHI Statistics

- Total number of incidents
- Number of incidents involving
  - Cyberattack
  - Ransomware
  - Unencrypted electronic equipment
  - Paper records
- Total number of individuals affected
Unauthorized Use of PHI

- Total number of incidents
- Number of incident involving
  - Electronic systems
  - Paper records
- Total number of individuals affected
Unauthorized Disclosure of PHI

- Total number of incidents
- Number of incident involving
  - Misdirected faxes
  - Misdirected emails
- Total number of individuals affected
What happens if you breach privacy?

• Investigation by Commissioner
• Orders including:
  • Undertakings
  • Publication
  • Fines
• Lawsuits including Damage awards
• College disciplinary proceedings
Liability for Invasion of Privacy

Intrusion Upon Seclusion

• In the January 2012 decision *Jones v. Tsige*, the Ontario Court of Appeal recognized a right to bring a civil action for damages for the invasion of personal privacy: “Intrusion Upon Seclusion”
Liability for Invasion of Privacy

Facts

• Jones and Tsige were both employees of Bank but did not know or work with each other
• Tsige became involved with Jones’ former partner, and became involved in a financial dispute with him
• Tsige accessed Jones’ bank records (including personal and transaction information) 174 times to determine if partner was paying support to Jones
• Jones complained and bank investigated.
Liability for Invasion of Privacy

Findings

• Even though Tsige never published the information or caused Jones any actual harm, Jones sued Tsige for invasion of privacy

• Trial Court dismissed the action on the basis that there was no free-standing right to privacy and that privacy legislation covered any breach

• Court of Appeal overturned dismissal of action and granted judgment to Jones for $10,000
Liability for Invasion of Privacy

Elements of the New Tort

• Defendant’s conduct must be intentional or reckless
• Defendant must have invaded plaintiff’s private affairs or concerns
• Reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish
Unless financial loss is proved, damages are limited to $20,000 based on five factors:

1. The nature, incidence and occasion of the defendant's wrongful act
2. The effect of the wrong on the plaintiff's health, welfare, social, business or financial position
3. Any relationship, whether domestic or otherwise, between the parties
4. Any distress, annoyance or embarrassment suffered by the plaintiff arising from the wrong and
5. The conduct of the parties, both before and after the wrong, including any apology or offer of amends made by the defendant
Plaintiffs alleged that 280 patient records of the Peterborough Regional Health Centre were improperly accessed and given to third parties, without the patients’ consent.

IPC investigated, but decided to take no further action against the Hospital.

Plaintiffs brought action for the tort of intrusion upon seclusion or breach of privacy.

Hospital conceded that the records were improperly accessed and apologized to the plaintiffs.

Hospital brought motion to dismiss the plaintiffs’ action, asserting that it disclosed no reasonable cause of action.
Hopkins: Findings

- Court rejected the Hospital’s arguments that PHIPA is a complete code that precludes private action for breach of privacy.
- Held that “the tort of breach of privacy, as alleged in the plaintiff’s statement of claim is a claim that should be allowed to proceed.”
- Hospital appealed to Court of Appeal, who unanimously upheld the lower court’s decision that PHIPA does not preclude a private plaintiff (or class plaintiff) from pursuing an action in tort against a health care institution for a privacy breach.
- Commissioner intervened, siding with the plaintiffs, and stating that its main objective is to address systemic issues rather than to provide individual remedies to complainants.
- Leave to appeal to the Supreme Court of Canada was denied.
Hopkins: Lessons Learned

- Private plaintiffs may pursue claims in tort for privacy breaches in the health care sector (have to wait for trial to see if in this case, claim will be successful)
- Claims may be pursued even if the IPC has taken no action
- Legal exposure for privacy claims faced by HICs has increased
- Breach of PHIPA requires proof of actual harm, while intrusion upon seclusion does not, but without actual proof, damages minimal
Lessons Learned from Privacy Breaches and IPC Orders
Orders Under PHIPA

Order 1:
Failures to manage PHI Records
Health Order No. 1: Facts

- The Commissioner was advised by a member of the media that health records were strewn across downtown Toronto as part of a film set recreating the 9/11 disaster.
- The film company had no knowledge that the papers it had purchased from a recycling company were actually health records, intended to be shredded.
Health Order No. 1: Order

• The clinic was ordered to do the following:
  • review its practices re secure storage of PHI
  • put in place a written agreement with any agent it retains to dispose of PHI which sets out obligation for secure disposal
• For all custodians, written agreements with any third parties who shred, recycle, store, dispose of or transmit any PHI
  Records must require third party to:
  • accept obligation to shred securely and irreversibly and provide an attestation of destruction;
  • transfer records securely, safeguarding the PHI contained therein
Orders Under PHIPA

Orders 2, 10, 13:
Unlawful Access to PHI Records
Health Order No. 2: Facts

- Patient admitted to Ottawa Heart Institute under maiden name to prevent estranged husband (employee at hospital) and his girlfriend (nurse at hospital) from having knowledge of her admission.
- Nurse accessed patient’s PHI records repeatedly; husband communicated information from hospital record.
- Patient complained; privacy officer ordered investigation.
- Discipline meeting scheduled weeks later; nurse repeatedly accessed patient’s PHI records in the interim.
Health Order No. 2: Findings

- Hospital had not taken steps that were reasonable in the circumstances to ensure that the personal health information was protected against theft, loss and unauthorized use or disclosure
- Hospital was ordered to review its practices and procedures to ensure that human resource issues did not trump privacy
- Hospital was ordered to implement a protocol that would require immediate steps to be taken upon being notified of an actual or potential privacy breach
Health Order No. 2: Lessons

- Hospital criticized for not taking steps to prevent ongoing privacy breaches by an employee, even after the hospital became aware that such breaches had occurred repeatedly.
- Hospital staff did not recognize the obvious threat to privacy posed by the estranged husband and his girlfriend—both employees of the hospital.
- Staff only recognized the threat to the physical security of the patient, not the threat to her privacy.
- After learning about the breach, the hospital was more concerned about the employee’s right to due process (Human Resources Policy) than the patient’s right to privacy.
- Hospitals can have both—but HR cannot trump privacy.
Health Order No. 10: Facts

• History: Same hospital involved in Health Order No. 2 (HO-002 in 2006) which showed that the hospital’s policies and procedures failed to prevent ongoing privacy breaches by an employee

• In 2010, employee disregarded a sensitive warning flag that popped up on computer screen while accessing patient files

• Hospital concluded employee was not authorized to view records. Employee received three days suspension without pay, plus privacy training and counseling

• Complainant received letter from hospital including apology and the audit results, nothing about employee discipline
Health Order No. 10: Findings

- Hospital had a satisfactory privacy policy as written, but failed to put their own standards into practice.
- Employees who were health care providers were given far too much access to patient documents.
- Technological restrictions on access were not effective.
- When breach did occur, hospital did not properly inform patients of the result of their investigation and did not file report with regulatory college.
Health Order No. 13

- Two hospital employees in clerical positions at Rouge Valley Health System (RVHS) used and/or disclosed the PHI of mothers who had recently given birth for the purpose of selling or marketing RESP.
- After discovering the privacy breaches, RVHS notified more than 14,000 new mothers that their PHI may have been unlawfully used and reported the breaches to the IPC.
- IPC conducted a thorough review of the incidents and RVHS’s privacy policies, practices and procedures.
• IPC found that RVHS did not take steps that were reasonable in the circumstances to safeguard PHI and did not have information practices in place that complied with PHIPA

• IPC identified the following deficiencies in RVHS’s approach to the protection of its patients’ PHI:
  • failed to implement sufficient technical measures to permit audits of user activities on its electronic PHI system;
  • inadequate privacy policies, procedures and information practices; and
  • failed to implement appropriate privacy training and awareness programs for its agents/employees.
Health Order No. 13

- IPC ordered that RVHS
  1. Implement measures to ensure that it can audit all electronic access by agents to PHI;
  2. Review and revise its existing privacy policies, ensure its Privacy Audits policy complies with same;
  3. Develop and implement a Privacy Training Program policy, a Privacy Awareness Program policy, and a Privacy Breach Management policy;
  4. Immediately review and revise its privacy training tools and materials; and
  5. Immediately conduct privacy training for all agents of the Hospital – including those in clerical positions.
Orders 4 & 7:
Management of Electronic PHI Records: Encryption is Key
Health Order No. 4: Stolen Laptop

• Health Order No. 4(HO-04) resulted from a hospital not having adequate policies and procedures to permit compliance with PHIPA

• In spite of the known high risk of loss or theft, extremely sensitive personal health information was transported on a portable device (laptop) without adequate safeguards

• This is clearly unacceptable, more than two years after PHIPA came into force

• Safeguards would include encryption, or better still, maintaining PHI on a secure server accessible remotely
Health Order No: 7
Lost USB Stick

• Order resulted from a USB memory stick, containing PHI of over 80,000 people, that was lost by a public health nurse
• Memory stick was not encrypted and person who issued stick did not know this was a requirement
• Found to be completely unacceptable in light of Order No: 4
• Act requires HIC to take reasonable steps to ensure PHI protected from theft, loss and unauthorized use and to ensure that PHI is retained and disposed of in a secure manner
• Also concern that they collected too much information (i.e. health card number when everyone was entitled to H1N1 shot, regardless of OHIP status)
PHIPA Decision No. 70: Facts

- Long-term care home reported privacy breach to IPC
- Employee had taken home records relating to two prospective residents
- Forgotten on public transit
- Home did not permit employees to take files home
- Employee had done so because of workload issues and inexperience
Response to Breach

- Notified individuals
- Contacted public transit authority
- Provided additional time management and privacy training to employee
- Revised initial staff training to strengthen privacy training
- Amended health care records policy to:
  - Clarify that staff cannot remove files from facility without permission
  - Limit printing to only when necessary
IPC Findings

• IPC found that home had not done enough to prevent breach
  • Policies and confidentiality agreements should have clearly prohibited removal of health records from the facility
• IPC found that home’s actions after the breach had adequately addressed the issue
• Determined no further action was necessary
Lessons Learned

• Staff training and policies important to proper safeguarding of PHI

• Response after breach occurs can help to reduce potential negative consequences
• Public hospital report of breach
• Registration clerk accessed records of high profile patient and 443 other patients
• Breach was detected in pro-active audit conducted in relation to media attracting patient
IPC Findings

• Scope and circumstances of breach gave rise to concern that hospital did not take reasonable steps to safeguard information

• IPC determined the hospital had taken reasonable steps to protect PHI in light of
  • Administrative Measures or Safeguards
  • Technical Measures or Safeguards
Administrative Safeguards

• Hospital had detailed breach management protocol that addressed containment, notification, and investigation
• Protocol recently revised to provide more detailed policy on disciplinary actions as a result of privacy breaches
• Confidentiality agreement with employee clearly prohibited the conduct engaged in
Administrative Safeguards

• When accessing patient electronic health records, agents receive a “pop up” warning clearly stating that patient information is permitted ONLY for the purposes of providing health care

• Agent must then click “Agree” to continue

• Thorough privacy training for new employees

• In response to this breach, hospital sent out staff-wide email on importance of privacy and snooping as a violation of PHIPA
Technical Safeguards

• Different levels of employees had access to different types of PHI as necessary
• Auditing system permitted hospital to determine who had accessed PHI
• But not what type of PHI
• Limitation on audits did not prohibit detecting this breach, but could hinder detection of future breaches
• Recommended future audit system include this feature
Lessons Learned

• Consideration of special risks (e.g. media attracting patient) can be very helpful

• Breaches can occur even where strong safeguards are in place

• Employee prosecuted and fined $10,000 – breaches can carry serious consequences
Questions
Lonny J. Rosen, C.S.*
Rosen Sunshine LLP
212 Adelaide Street W, Suite 200
Toronto, Ontario
M5V 2E2

Tel.: (416) 223-4222
E-mail: rosen@rosensunshine.com
Website: http://www.rosensunshine.com

* Certified by the Law Society of Upper Canada as a Specialist in Health Law