A Privacy Update for Regulated Health Professionals 2023

Twitter: @katedewhirst

This is not legal advice. This is for general information purposes only.

Overview

1. Role of a HIC
2. Circle of care
3. Privacy and social media
4. Privacy and kids
5. Privacy breach identification

Handouts

1. These slides
2. The Privacy Prescription: 14 basic steps for privacy compliance for health practices
3. Summary of the Information and Privacy Commissioner's decisions in health privacy
4. Ontario Caregiver Organization, FAQs re Children and Youth and Privacy and Consent

Topic 1

Role of a Health Information Custodian

Are you a Health Information Custodian (HIC)?

Are you an agent?

Health information custodians (HICs)

- Health care practitioners
- Public and private hospitals
- Psychiatric facilities
- Independent health facilities
- Community health or mental health centres, programs or services
- Long-term care homes
- Placement coordinators
- Retirement homes
- Pharmacies
- Laboratories
- Specimen collection centre
- Ambulance services
- Operators of care homes (residential tenancies)
- Homes for special care
- Community support services provider
- Medical Officer of Health
- Ontario Agency for Health Protection and Promotion
- Ontario Air Ambulance Services
- LHIN (Home and Community Support Services)

If you have your own practice you are a health information custodian

If you work in a group - you have to decide whether there is a single custodian or multiple custodians

If you are employed at a hospital, family health team, birth centre, corporation, or a community health centre - you are likely an "agent" - where your employer is the custodian and you follow the employer's privacy rules

13 Key HIC Responsibilities

1. Choose a privacy contact person (privacy officer):
   - Respond to access and correction requests
   - Respond to inquiries about the HIC's information practices
   - Receive privacy complaints
   - Ensure overall PHIPA compliance
2. Make records available to clients (including electronic health records available to clients in electronic formats)
3. Have clear rules about privacy (usually in policy)
4. Ensure all agents are informed about their duties under PHIPA (training + confidentiality pledges annually)
5. Have a written statement available to the public about information management practices

13 Key HIC Responsibilities

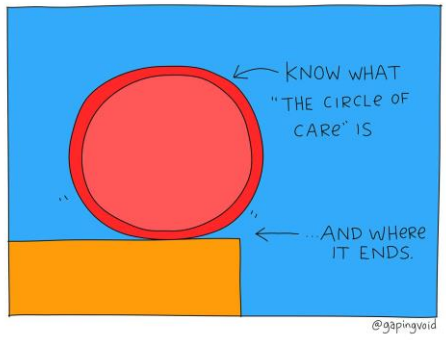
6. Ensure protection of PHI against loss, theft, unauthorized access, use or disclosure, copying, modification, disposal (ensure technical, physical and administrative safeguards are in place and conduct audits and privacy impact assessments/threat risk assessment)
7. Ensure that records are retained, transferred and disposed of in a secure manner
8. Ensure appropriate privacy expectations and content in vendor agreements
9. Perform audits of electronic health records
10. Ensure new information systems comply with digital asset interoperability standards
11. Notify impacted individuals PHI is stolen, lost or accessed by an unauthorized person
12. Complete annual statistical reporting to the Information and Privacy Commissioner of Ontario and if there are reportable breaches in the moment
13. Obtain insurance to protect yourself and your practice from cyber risk

Recent increased PHIPA compliance

- ✓ Annual statistical reporting to IPC since 2019 and in moment reporting of certain breaches
- ✓ Increased fines to $200,000 and $1 million + jail time in 2020
- ✓ New interoperability standards for all new software after 2021 (approved virtual visit vendor platforms – OH)
- ✓ Proposed additional auditing requirements estimated to come 2023
- ✓ Changing standards for clients having electronic access to their own records in electronic format
- ✓ Changing standards to acknowledge the roles of OHTs and explaining system integration to the public
- ✓ Changing IPC standards for safeguards for virtual care, working from home, secure destruction

Topic 2

Circle of Care



Circle of Care

When the client wants their information shared with their other health care providers so they can provide health care – can be done assuming implied consent

Lockbox – Consent Directive

When the client does not want their information shared with their other health care providers – that is a lockbox request

1. WHO: Disclosing to (or receiving from) a direct health care provider AND
2. WHY: For providing or assisting in providing health care

Who can be in circle of care?

1. School
2. Hospital
3. Insurance company
4. Client's sister
5. Landlord
6. Police
7. Primary care team
8. WSIB
9. CAS

IN	OUT
Hospital	School
Primary care team	Client's sister
	Landlord
	Police
	WSIB
	CAS
	Insurance company

In Circle of Care =
Can share with implied consent

- Health care practitioners
- Public hospitals
- Private hospitals
- Psychiatric facilities
- Independent health facilities
- Community health or mental health centres, programs or services
- Long-term care homes
- Placement coordinators
- Retirement homes
- Pharmacies
- Laboratories
- Specimen collection centre
- Ambulance services
- Operators of care homes (residential tenancies)
- Homes for special care
- Community support services provider
- Medical Officer of Health
- Ontario Agency for Health Protection and Promotion
- Ontario Air Ambulance Services
- LHIN (Home Care and Community Support Services)

NOT in the Circle of Care =
Must have express consent OR otherwise be permitted or required by law to disclose

- Insurance companies
- Employers
- Family members
- Teachers and Schools (except school board nurses, social workers, psychologists, speech-language pathologists, OTs, PTs, audiologists etc. are in)
- Landlords
- Children's Aid
- Police
- Health Canada
- MoH or MLTC
- Prayer or Spiritual healers and leaders

How do you know you can share information with external health care providers relying on **IMPLIED CONSENT**?

You can ASSUME it

Please share!

But if you think your client would not want their information shared – ask your client first.

Circle of care is not NO consent

If your client objects then you cannot share the information relying on implied consent

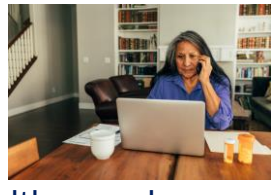
Going forward you will need express consent – unless you are permitted or required by law to share

Ontario Health Teams

Connecting Care Act, 2019 – now moving us into new world order where health care providers will share PHI within a geographic region

BUT clients must be told about this in posters, brochures and community notices

Mature OHT Status



- ✓Integrated health records
- ✓Client portals with whole health history

Topic 3

Social Media

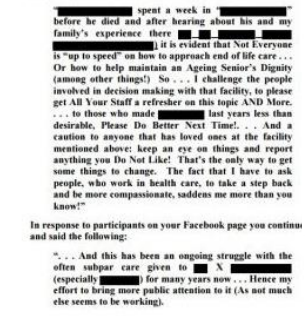
Cautionary Tale: Dr. 6ix, 2021

Cosmetic surgeon received 6 month license suspension from CPSO

- Video surveillance
- Social media
- Live media recording

Cautionary Tale: Papadopolous, 2012

- Psychologist gave advice on an online podcast
- She promoted a concept of "deFOOing" which was found to violate the College standards of practice
- Question: Are you engaged in a clinical relationship online?



"[redacted] spent a week in "[redacted]" before he died and after hearing about his and my family's experience there [redacted] it is evident that Not Everyone is "up to speed" on how to approach end of life care . . . Or how to help maintain an Ageing Senior's Dignity (among other things!) So . . . I challenge the people involved in decision making with that facility, to please get All Your Staff a refresher on this topic AND More. . . . to those who made [redacted] last years less than desirable, Please Do Better Next Time!. . . And a caution to anyone that has loved ones at the facility mentioned above: keep an eye on things and report anything you Do Not Like! That's the only way to get some things to change. The fact that I have to ask people, who work in health care, to take a step back and be more compassionate, saddens me more than you know!"

In response to participants on your Facebook page you continu and said the following:

". . . And this has been an ongoing struggle with the often subpar care given to [redacted] X [redacted] (especially [redacted]) for many years now . . . Hence my effort to bring more public attention to it (As not much else seems to be working).

Cautionary Tale: Strom 2020

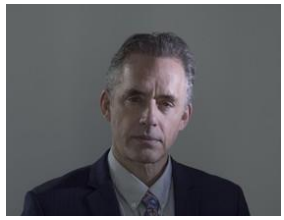
As an RN and avid health care advocate myself, I just HAVE to speak up! Whatever reasons/excuses people give for not giving quality care, I Do Not Care. It. Just. Needs. To. Be. Fixed. And NOW!"

You continue on your Facebook page as follows:

". . . "Why do you do your job?" "Do you actually care about the people you WORK FOR/Care For?" "Or is it JUST A JOB, WITH A PAYCHEQUE?" . . . If so, maybe it's time to take a step back.
Either way I just want [redacted] (and everyone else in that facility) to be treated well, ALWAYS!"

2016 Saskatchewan Nurse found guilty of professional misconduct by regulator
Overturned in Court of Appeal decision
2020 Strom v. Saskatchewan RNA

Cautionary Tale: Dr. Peterson, 2023 Twitter



Psychologist is being required to take "social media training" after making comments on Twitter that

- Lack professionalism
- Bring the profession into disrepute

Photo: National Post

Topic 4

Privacy and Kids

Test for Capacity

Must be ABLE to understand BOTH

1. The information about the decision
2. The reasonably foreseeable consequences of saying yes or no

The clinician providing care determines capacity

Who may consent

1. A "capable" client – of any age

2. If a client is "incapable" – their substitute decision-maker

3. If a client is deceased
   If there is a will = executor
   If no will = administrator of estate

Who may consent

4. If a capable client is under the age of 16, a parent can ALSO consent to privacy decisions

UNLESS decision relates to information about

- **Treatment child decided on own**
- **Counseling child did on own**

AND

If there is a dispute between a capable client and a parent – the capable client's choice wins

AGE	CAPACITY	DECISION MAKER
Person of any age	If capable	Can make decisions about release of everything in their own health record
Person of any age	If incapable	Needs a substitute decision-maker to release anything in health record
Under age of 16 (birth to 16 less a day)	If capable	Can make decisions about release of everything in their own health record AND A parent (or CAS) can also consent to release of information about any treatment or counseling that child did not consent to on their own BUT NOT IF THE CAPABLE CHILD OBJECTS TO PARENT MAKING SUCH DECISIONS

Quiz

Can child consent? Can parents consent?

13 year old capable of making decisions – parents want historic records from when client was 9 and had services with parental consent

(does answer change if child is 16?)

Quiz

Can child consent? Can parents consent?

8 year old child incapable of making decisions - parents want a copy of the health record to get a second opinion

Quiz

Can child consent? Can parent consent?

15 year old received services on their own – parents want a copy of the record to send to insurance company

Parental Disputes

For an incapable kid, the parents together make decisions about treatment and privacy

UNLESS

that right has been removed from one or both of them

List of Substitute Decision-Makers

(PHIPA, s. 26)

LEGAL

1. Guardian of the person
2. Attorney for personal care or property
3. Personal representative appointed by CCB

FAMILY - AUTOMATICALLY

4. Spouse or partner
5. Parent or CAS (not access parent; and not parent if CAS has authority)
6. Access parent
7. Brother or sister
8. Any other relative

SDM of LAST RESORT

9. Public Guardian and Trustee

If there is a separation or divorce - assume joint custody unless shown otherwise

- Court order
- Separation agreement approved by court

Decision 160: Parent Access

Joint custodial parent (Parent A) made an access request for health records of his kids.

The other joint custodial parent (Parent B) refused.

IPC concluded: If 2 SDM parents and one parent objects – can't give access to information to the other.

No need to canvass both parents (unless you believe the other SDM would disagree)

"...there is no obligation in every case for a custodian faced with a request from a SDM to canvass the views of all equally ranked SDMs in order to satisfy itself that they all agree to the request. ... a custodian is generally entitled to rely on an assertion by a person claiming to be the lawfully authorized decision-maker for an individual. However, where ...there is reason to believe that another equally ranked SDM would disagree...the custodian would not be entitled to rely on such an assertion. In such a case, the HIC would be entitled to refuse the request."

Polyamorous Parents

April 2021 a BC judge ordered second mother declared a third parent to a child of a polyamorous trio

Topic 5

Privacy Breach Identification

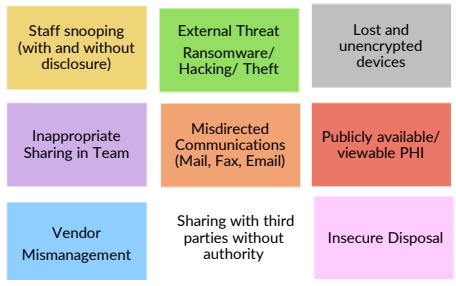
Safeguards

You have to protect client information and client records from:

- Loss
- Theft
- Unauthorized use and disclosure
- Unauthorized modification or destruction

And if there is a breach, you have to notify clients + IPC

9 Privacy Breach Categories



IPC Privacy Breach Protocol

IPC has a specific page dedicated to helping HICs "Responding to a Privacy Breach"

- Privacy Breach Protocol
- Potential Consequences of a Breach under PHIPA

IPC: What to do when faced with a privacy breach

IPC Protocol

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

Must Read: What to do when faced with a privacy breach: Guidelines for the health sector

2 Types of Breach Reporting to IPC

1. Annual
2. In the moment

Annual Report on Numbers and Statistics

 # times PHI was stolen

- by an internal party
- by a stranger
- by a ransomware attack or other cyber attack
- on an unencrypted portable electronic device
- in paper format

 # times PHI was lost

- due to ransomware attack or other cyber attack
- on an unencrypted portable electronic device
- in paper format

 # times PHI was used without authority

- through electronic systems
- though paper records

 # times PHI was disclosed without authority

- through misdirected faxes
- through misdirected emails

 # times PHI was collected without authority by means of EHR

11,263 breaches reported in 2021

- 55% hospitals
- 12% lab or specimen collection centre
- 7% health care practitioner or group practice
- 7% community health or mental health centre
- 4% LHIN
- 4% pharmacy
- 3% public health
- 2% independent health facility
- 1% ambulance
- 1% home care and community care
- .5% long term care

11,263 breaches

51 theft

252 lost records

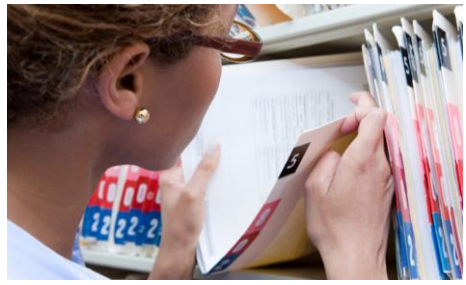
1,495 unauthorized use

9,445 unauthorized disclosure

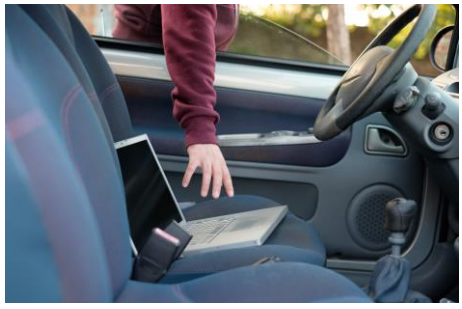
4,848– misdirected faxes

1,165 misdirected emails

7 activities you must report to IPC ASAP



1. Snooping



2. Stolen

3. Go public

4. Pattern of breaches

5 and 6. Took discipline

7. "Significant"

Need more privacy support?

1. Free monthly "Ask me Anything about health privacy" – first Wednesday of every month (not in the Summer)
2. Free summary of all health privacy decisions of the IPC
3. College Guidelines on Privacy, Telehealth, Recordkeeping, Social Media
4. IPC resources for Health Sector