Kate Dewhirst
BRINGING THE LAW TO LIFE

A Privacy Update for Regulated Health Professionals

Twitter: @katedewhirst
Facebook:
Kate Dewhirst Health Law

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

Overview

1. Privacy lingo
2. Recent updates to privacy law in Ontario
3. Safeguards, prevention and privacy breach reporting
4. Audience Questions

Handouts

1. These slides
2. Visual summary of privacy training
3. The Privacy Prescription: 11 basic steps for privacy compliance for health practices
4. Summary of the Information and Privacy Commissioner's decisions in health privacy

Topic 1

Privacy Lingo

Are you a Health Information Custodian (HIC)?

Are you an agent?

Health information custodians (HICs)

- 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 (under *Home Care and Community Services Act, 1994)*
- Medical Officer of Health
- Ontario Agency for Health Protection and Promotion
- Ontario Air Ambulance 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, 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

Personal Health Information (PHI)

Personal Health Information

Is identifying information about someone's:

- Physical or mental health (family history)
- Care provided and name of health care provider (name of agency/organization/business)
- Health number
- Body parts or bodily substance or tests or exams
- Substitute Decision Maker's name

Is it PHI?

- Emails to patients
- Emails between colleagues
- Text messages
- Voice messages
- Handwritten notes
- Quality improvement reports
- Complaints documentation and responses
- Risk management forms
- Referral information about someone not yet a patient
- Fax from another clinician about a patient
- Research database
- Appointment book/online schedule
- Scrap notes
- Video surveillance tapes

"In play"

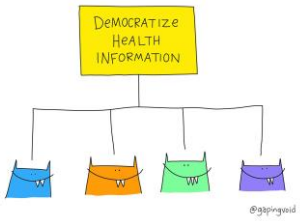
1. Have to protect it
2. Must provide access to it

Topic 2

Recent changes to privacy law in Ontario

We've had PHIPA since 2004
There were major changes in 2019 and 2020

PHIPA Modernization



Ontario Health + THE provincial eHR

Mandatory logging and auditing of activity in health records (details not yet in force)

Audits are an essential technical safeguard to protect personal health information. They can be used to deter and detect collections, uses and disclosures of personal health information that contravene PHIPA. In this way, they help to maintain the integrity and confidentiality of personal health information stored in electronic information systems.

Commissioner Beamish, H0-013

PHIPA - new s. 10.1 E-audit log

10.1 (1) Subject to any prescribed exceptions, a health information custodian that uses electronic means to collect, use, disclose, modify, retain or dispose of personal health information shall,

(a) maintain, or require the maintenance of, an electronic audit log described in subsection (4);

(b) audit and monitor the electronic audit log as often as is required by the regulations; and

(c) comply with any requirements that may be prescribed. Access by Commissioner

PHIPA - new s. 10.1 E-audit log

Content of log

(4) The electronic audit log must include, for every instance in which a record or part of a record of personal health information that is accessible by electronic means is viewed, handled, modified or otherwise dealt with,

(a) the type of information that was viewed, handled, modified or otherwise dealt with;

(b) the date and time on which the information was viewed, handled, modified or otherwise dealt with;

(c) the identity of all persons who viewed, handled, modified or otherwise dealt with the personal health information;

(d) the identity of the individual to whom the personal health information relates; and

(e) any other information that may be prescribed.

Digital asset interoperability

Increased penalties, fines and powers of the IPC

Topic 3

Safeguards, Prevention and Breach Management

Prevention - Security Basics

Safeguards Principle

Personal health information must be protected by security safeguards appropriate to the sensitivity of the information

Safeguards

You have to protect patient information and patient records from:

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

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

Safeguards

You have to ensure that your records are retained, transferred or disposed of in a secure manner

Safeguards

If you keep records at a patient's home (or anywhere else) – those records have to be protected and with consent of patient.

Not a standard of perfection

Standard of Reasonableness

#1 Safeguarding personal health information
#10 Secure destruction of personal information
#12 Encrypting personal health information on mobile devices
#13 Wireless communication technologies: video surveillance systems
#16 Health-care requirement for strong encryption
#18 Secure transfer of personal health information
#19 Communicating Personal Health Information by Email
Protecting Against Ransomware
Disposing of your Electronic Media
Avoiding Abandoned Health Records
Protect Against Phishing
Working from home during the COVID-19 pandemic
Privacy and security considerations for virtual health care visits

Convenience does not trump privacy

Reminders in Shared Spaces

- Don't leave your computer logged on just because logging back in takes time
- Don't use an unattended computer because it's quicker than going to another and logging in as yourself
- Don't open the full chart when the demographics screen has all the information you need

Passwords

- Don't share passwords
- Have a different password professionally than personally

2 Risky Activities

1. Clicking a link
2. Opening an attachment

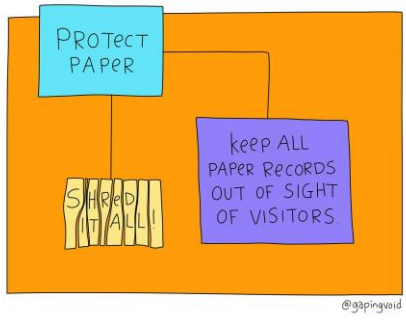
New IPC guidance document July 2020

Working from Home

1. Take care that people with whom you share space cannot see or overhear the virtual visits
2. Avoid printing documents with personal health information at home
3. Check for temporary downloads
4. Lock device or sign out of the EHR or remote desktop on any shared devices
5. Segregate electronic work files from family files

* Staff should be allowed to block their personal numbers if they want to do so

Don't



Virtual Visits

Visit between a clinician and a patient using technology to deliver a health care service or assessment (not in person)

New IPC guidance document February 2021

Remember to check your College guidelines on virtual care or telehealth

Modalities

Telephone consults

Videoconferencing

Secure messaging

10 Tips Videoconferencing

1. Best practice means that both you and patient join videoconference from a private location using a secure internet connection (not public WiFi)
2. Enclosed soundproof room – or otherwise quiet and private place with window coverings
3. Use headphones rather than speaker
4. Watch where screens are positioned
5. Address accessibility concerns regarding captioning or screen readers

10 Tips Videoconferencing

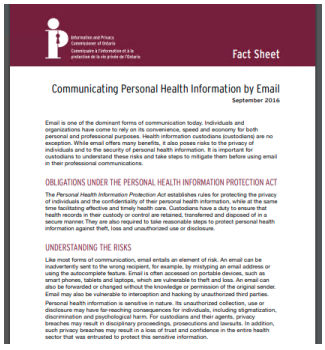
6. Ensure meeting is secure from unauthorized participants
7. Do not record meeting unless express consent
8. HIC introduce themselves and anyone else present and ensure consent to their involvement
9. Ask if anyone is accompanying the patient and confirm consent of patient
10. Use high-quality sound and resolution to collecting information including verbal and non verbal cues

Email

Nothing illegal or inappropriate about using email to communicate … BUT …

You must take "reasonable steps" to ensure all PHI is protected always

IPC guidance document 2016



Fact Sheet

Communicating Personal Health Information by Email

September 2016

Email is one of the dominant forms of communication today. Individuals and organizations have come to rely on its convenience, speed and economy for both personal and professional purposes. Health information custodians (custodians) are no exception. While email offers many benefits, it also poses risks to the privacy of individuals and to the security of personal health information. It is important for custodians to understand these risks and take steps to mitigate them before using email in their professional communications.

OBLIGATIONS UNDER THE PERSONAL HEALTH INFORMATION PROTECTION ACT

The *Personal Health Information Protection Act* establishes rules for protecting the privacy of individuals and the confidentiality of their personal health information, while at the same time facilitating effective and timely health care. Custodians have a duty to ensure that health records in their custody or control are retained, transferred and disposed of in a secure manner. They are also required to take reasonable steps to protect personal health information against theft, loss and unauthorized use or disclosure.

UNDERSTANDING THE RISKS

Like most forms of communication, email entails an element of risk. An email can be inadvertently sent to the wrong recipient, for example, by mistyping an email address or using the autocomplete feature. Email is often accessed on portable devices, such as smart phones, tablets and laptops, which are vulnerable to theft and loss. An email can also be forwarded or changed without the knowledge or permission of the original sender. Email may also be vulnerable to interception and hacking by unauthorized third parties.

Personal health information is sensitive in nature. Its unauthorized collection, use or disclosure may have far-reaching consequences for individuals, including stigmatization, discrimination and psychological harm. For custodians and their agents, privacy breaches may result in disciplinary proceedings, prosecutions and lawsuits. In addition, such privacy breaches may result in a loss of trust and confidence in the entire health sector that was entrusted to protect this sensitive information.

Plus IPC guidance document February 2021

FEBRUARY 2021

Privacy and security considerations for virtual health care visits

GUIDELINES FOR THE HEALTH SECTOR

The delivery of virtual health care has become an integral part of Ontario's health system. Virtual health care can include secure messaging, telephone consultation, and videoconferencing. These forms of digital communication offer significant convenience for health information custodians (custodians) and their patients where physical distance poses a challenge. However, virtual health care also raises unique privacy and security concerns because it depends on technologies, communication infrastructures, and remote environments. Virtual health care raises new kinds of cybersecurity risks that are not as prevalent in the analog world.

PHIPA applies to virtual care as it does to in-person care.

Ontario's health privacy law, the *Personal Health Information Protection Act (PHIPA)*, applies to virtual care as it does to in-person care. Custodians must comply with the provisions of *PHIPA*, in addition to all other applicable laws and regulations, as well as guidance issued by relevant professional regulators.

In this guide, we recall some of the key requirements in *PHIPA* relevant to all custodians, including those who operate in a virtual health care context. We then provide some practical steps custodians should take to protect personal health information, particularly as they plan and deliver virtual health care.

22 Tips Email + Secure Messaging

1. Only use professional accounts (not personal email address)
2. Patients should be registered through a secure messaging solution that authenticates their identity before accessing messages
3. Use encryption for emails to and from patients if PHI
4. Encrypt or password-protect document attachments
5. Share passwords through different channel or message
6. If unencrypted email system – assess risk of message, sensitivity, urgency

22 Tips Email + Secure Messaging

7. Verify identity of patient – send a test message in advance and ask for confirmation
8. Provide notice that the information received is confidential
9. Provide instructions to follow if message is received in error
10. Confirm address is up-to-date
11. Ensure address corresponds to intended address
12. Regularly check pre-programmed addresses

22 Tips Email + Secure Messaging

13. Restrict access to email system and content on need-to-know basis to team
14. Inform patients of changes to your address
15. Acknowledge receipt of emails
16. Minimize disclosure in subject lines and message content
17. Ensure strong access controls
18. Recommend patients use a password protected email address only they can access

22 Tips Email + Secure Messaging

19. If email goes into EHR – no need to keep email – so securely delete
20. Check to make sure email is going to the right recipient before sending
21. Do not send extra attachments by accident – check before you send
22. Be careful of "cc'ing" versus "bcc'ing" in bulk emails so not to identify patient lists and patient email addresses to other patients

Breach Management

9 Privacy Breach Categories

Staff snooping (with and without disclosure)	External Threat Ransomware/ Hacking/ Theft	Lost and unencrypted devices
Inappropriate Sharing in Team	Misdirected Communications (Mail, Fax, Email)	Publicly available/ viewable PHI
Vendor Mismanagement	Sharing with third parties without authority	Insecure Disposal

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

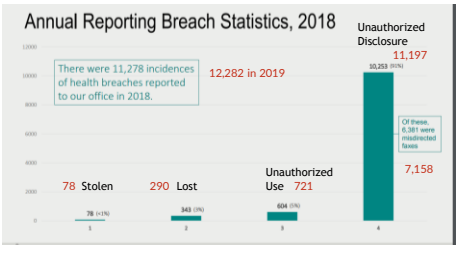
- due to ransomware attack or other cyber attack
- on an unencrypted portable electronic device
- in paper format

 # times PHI was used without authority

- through electronic systems
- though paper records

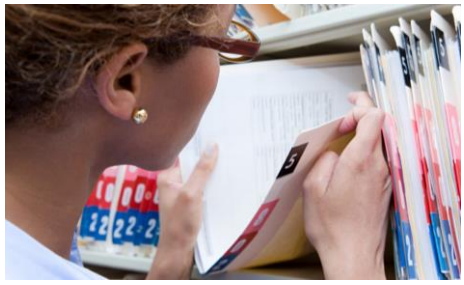
 # times PHI was disclosed without authority

- through misdirected faxes
- through misdirected emails

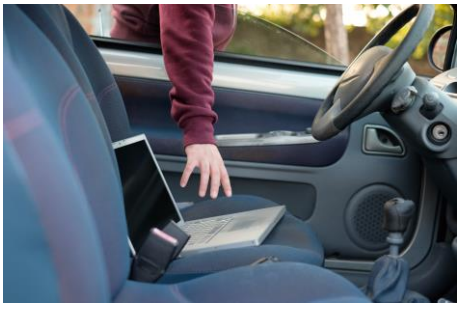


Information and Privacy Commissioner of Ontario, May 2020

7 activities you must report to IPC ASAP



1. Snooping



2. Stolen

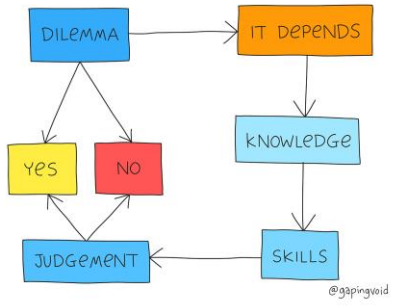
3. Go public

4. Pattern of breaches

5 and 6. Took discipline

7. “Significant”

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



Audience Question

If both privacy legislations (PHIPA and PIPEDA) intersect in a health professional's practice, does one legislation supersede the other?

Audience Question

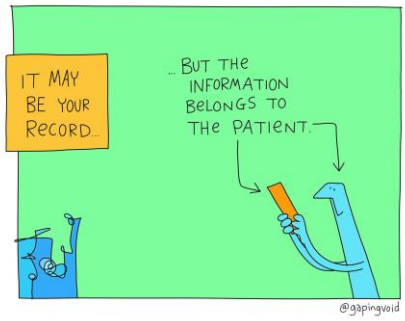
Are there any circumstances where PHIPA and PIPEDA can apply? Some health professionals collect both PI and PHI in assessments.

Audience Question

A patient wants me to destroy their records - is that allowed?

Audience Question

I am the health information custodian. If a patient requests their chart and it includes another professional's notes, should I disclose the whole chart?



Audience Question

A patient wants to video record the treatment session, can I refuse?

Audience Question

All the health professionals at my organization use the same password to upload reports. Is this a privacy issue?

Audience Question

I am providing virtual care. Is the paid version of Zoom PHIPA compliant? If not, what is?

Selecting a Virtual Visit Vendor

- Ontario Health's "Virtual Visits Solution Standard"
- Online list of "verified" platforms

Solution	Solution Version	Vendor	Video	Secure Messaging	Status Details
aTouchAway	v12.10.4 #fca5	Aetonix Solutions Inc.	Verified	Verified	
Adracare	5.15.0	Adracare Inc.	Verified	Verified	
OnCall Health	2.1	OnCall Health Inc.	Verified	Verified	
Maple	4.6.13 | 4082 | v33	Maple Corporation	Verified	Verified	
Telus PS Suite EMR	5.18.301 or higher	Telus Health Solutions Inc.	Verified	-	
Telus Med Access EMR	5.11 or higher	Telus Health Solutions Inc.	Verified	-	
TelAsk	5	TelAsk Technologies Inc.	Verified	Verified	
EMERGE	2.0	Emerge Virtual Care	Verified	-	
Banty Medical	3.0	Banty Inc.	Verified	-	
SigMail	v1.4.1491+20210413	Sigma Healthtech Inc.	-	Verified	

50+ additional platforms still being verified including Zoom, Teams

Audience Question

Can I assume a family doctor is always in the patient's circle of care?

Audience Question

If I am no longer employed in the auto sector, if called to court can I review the patient/client file without consent?

Audience Question

Is it permitted from a privacy perspective to provide personal health documents to WSIB for claims about a patient?

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. Privacy Officer Foundations training – next course starts September 2021
4. Team Training – I train you and your team about privacy
5. One-on-one – Customized privacy policies or assistance with privacy questions or breach response

https://katedewhirst.com for details

kate@katedewhirst.com