

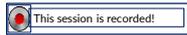
Kate Dewhurst
BRINGING THE LAW TO LIFE



Privacy for Compass Team Members

Twitter: @katedewhurst
Facebook:
Kate Dewhurst Health Law

zoom Platform



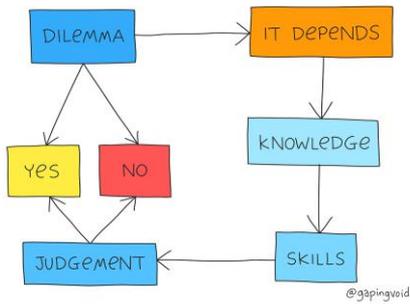
A copy of these slides is
available after the presentation



Overview

- 1. The meaning of privacy
- 2. Capacity and consent and sharing information with families
- 3. Safeguards and privacy breach response







Topic 1

The meaning of privacy





Confidentiality is one part

- Protect personal information in your care
 - Maintain its secrecy
 - Not wrongfully disclose
- = Your obligation







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)
- Health number
- Body parts or bodily substance or tests or exams
- Substitute Decision Maker's name



Is it PHI?

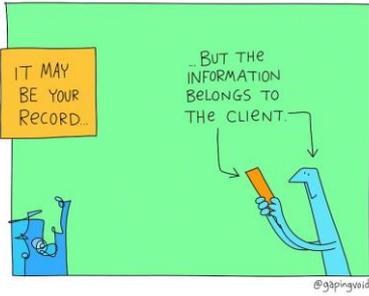
- ▶ Emails to clients
- ▶ Emails between colleagues
- ▶ Text messages
- ▶ Voice messages
- ▶ Handwritten notes
- ▶ Quality improvement reports
- ▶ Complaints documentation and responses
- ▶ Risk management forms
- ▶ Referral information about someone not yet a client
- ▶ Fax from another team about a client
- ▶ 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

Capacity and Consent



Quick Quiz

- Can you release information about a client who is over the age of 16 to their parents?
- Can you leave information on a voice message where other family members might hear the message?
- Can family members book appointments for their loved ones?

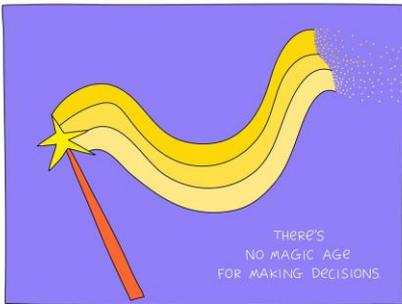


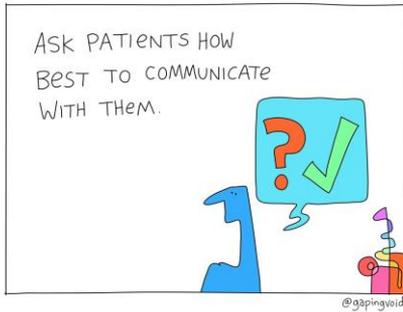
Uh oh... Privacy Paralysis



It depends







It depends ...

- ▶ Capacity
- ▶ What does your client want?
- ▶ Not an all or nothing option

Reminder:

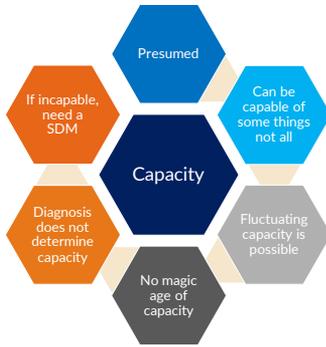
- ▶ No age of consent
- ▶ Some information may be shared with parents for kids under age 16 depending on what it is



Capacity - legal test for the mental ability to make decisions for oneself

Consent - act of giving permission for an activity





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



Quiz

Can child consent? Can parents consent?

13 year old capable of making decisions – school wants mental health records from when client was a young child

(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?

11 year old making own counseling decisions –
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



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

- ▶ Court order
- ▶ Separation agreement approved by court



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 <u>AND</u> A parent 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

Consent

Clients control their information (subject to some exceptions)

In order to collect, use or disclose personal health information, you must:

1. Have **consent** OR
2. Be **permitted** by law OR
3. Be **required** by law



Express Consent

Oral or Written

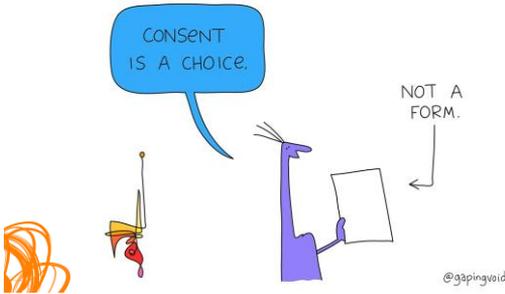
Implied Consent

Implied based on circumstances

No consent

"Permitted or required by law"





Withdrawing consent

A client can withdraw consent

- ▶ Orally or in writing
- ▶ At any time (but not retroactive)



Record a client's withdrawal of consent in the client's record

No Consent

If permitted or required by law



Permitted by law

If PHIPA or another law says you **MAY** collect, use or disclose personal health information without the consent of the client



PHIPA says you can use and disclose for certain purposes without consent, such as:

- Planning and delivering programs and evaluation
- System planning
- Quality, risk management, error management
- Obtaining payment, reimbursement, financial reporting
- Research (with REB approval)
- Proceedings



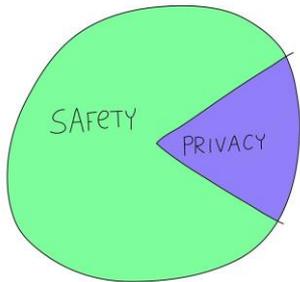
Your client cannot opt out of these unless your team permits

When you are permitted by law to act - be careful not to give the client a false choice

You can only do those activities if they are part of your job (Ask your supervisor)



DO NOT ENGAGE IN SELF-INITIATED PROJECTS IN THE CLIENT'S HEALTH RECORD



SAFETY
TRUMPS
PRIVACY
@gapingvoid

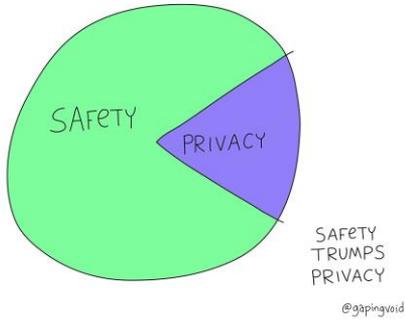
To reduce or eliminate a significant risk of serious bodily harm

Safety trumps privacy

Usually means calling police + Intended victims

Get Advice





Required by law

Sometimes a law or THE LAW says you **MUST** collect, use or disclose personal health information

When you are required by law to act – you do not get the client’s permission



Required to disclose under another law:

- ▶ A child in need of protection
- ▶ Public health concerns and communicable diseases
- ▶ Transportation safety
- ▶ Regulatory Colleges
- ▶ Coroners Act
- ▶ WSIB
- ▶ Missing persons



If **required by law** to disclose – ask the authority who is telling you to disclose to them to document that for you so you can add the requirement to the client’s record



Required to disclose by THE LAW:

- ▶ Court order
- ▶ Summons to witness
- ▶ Subpoena
- ▶ Warrant
- ▶ Urgent demand for record (missing person)



Quiz

What kind of consent?

Insurance company sends request for records and includes a consent form that is 1 year old



Quiz

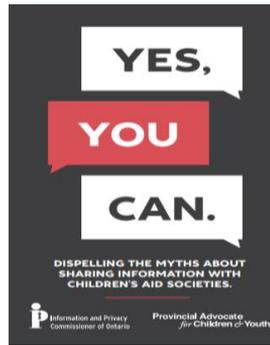
What kind of consent?

Children's Aid Society asks for a copy of your records



Children's Aid Society

- ✓ With express consent
- ✓ Share if they are substitute decision makers
- ✗ Not in circle of care
- ✓ Must report
- ✓ May disclose to assist their statutory duties



Part X - January 1, 2020

Child, Youth and Family Services Act, 2017



Quiz

What kind of consent?

School asks for mental health and counselling records to help with for an independent education plan



Quiz

What kind of consent?

Police ask you whether someone is a client of yours



Police



- X Not in circle of care
- ✓ Express consent
- ✓ To reduce or eliminate significant risk of serious bodily harm
- ✓ Mandatory if there is urgent demand for records for missing person or a court order or warrant/subpoena (tell your supervisor)
- ✓ Discretion to share if there is an investigation (tell your supervisor)



Situation Tables - VTRA

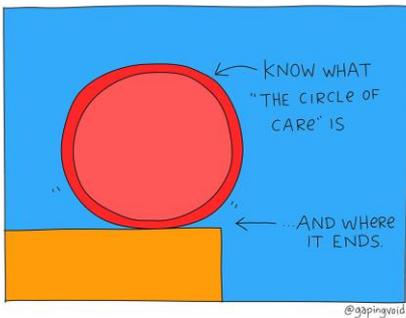


Is a lawyer "the law"?

You get a lawyer's letter telling you to send information about your client to them?

Must you?





Topic 3

Safeguards



Safeguards Principle

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



Safeguards

Your team has to protect client information and client records from :

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



And affected clients must be notified of a breach + IPC in some cases.

Not a standard
of perfection

Standard of
Reasonableness





Need to know

(Ask Yourself: do I need
this info to do my job?)





What hat are you wearing?

Mandatory Activities
 Provide care Scheduling
 Follow up Filing
 Consult

Encouraged Activity with Authorization by Role
 Quality improvement
 Learning and teaching
 Self Reflection

Prohibited Activity
 Snooping







Intrusion upon seclusion

1. Intentional intrusion (including "reckless")
2. Invaded private affairs without lawful justification
3. The intrusion would be considered **highly offensive to a reasonable person**
4. Causing distress, humiliation or anguish (although the Court suggests this last one will be assumed when the first three are satisfied) - no need to prove actual harm





Rouge Valley Health System

Intrusion upon seclusion

1. Intentional intrusion (including "reckless")
2. Invaded private affairs without lawful justification
3. The intrusion would be considered **highly offensive to a reasonable person**
4. Causing distress, humiliation or anguish (although the Court suggests this last one will be assumed when the first three are satisfied) - no need to prove actual harm





New IPC guidance document February 2021



Virtual Visits

Providing medical or clinical services by telephone, video or live text meeting

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

Virtual Care

Secure messaging

Telephone consult

Videoconferencing

Only view the minimum amount of information relevant to the work you are doing and your role in the organization





Verify the identity of your client + send test messages + test with photo



if possible, use work email accounts rather than personal ones for work-related emails involving personal data

before sending an email, check that you're sending it to the correct recipient, particularly for emails involving personal data

make sure nothing EXTRA attached

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





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





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 record 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





Privacy considerations when working from home:

1. Take care that people with whom you share space cannot see or overhear your 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



if using portable storage devices, such as USBs and portable hard drives, ensure they are encrypted and password protected

keep your software up-to-date with anti-virus protection

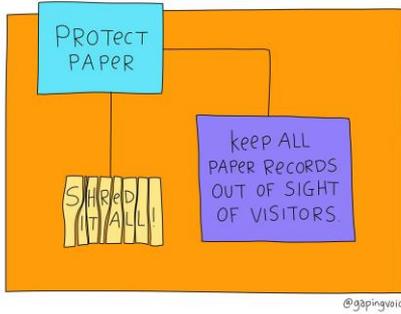
Set default settings to most privacy protective

Paper matters too



Don't







Don't





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 used without authority

- ▶ through electronic systems
- ▶ through paper records

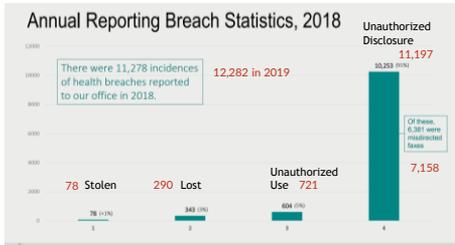
times PHI was lost

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

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





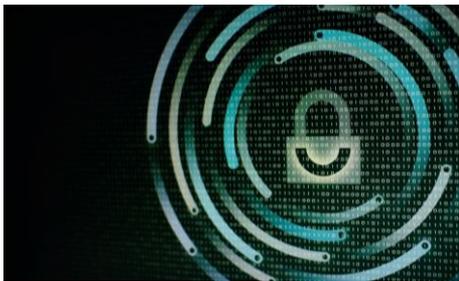
2. Stolen





3. Go public





4. Pattern of breaches

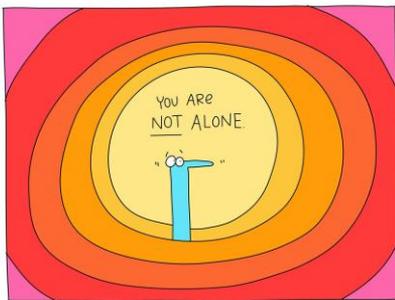




5 and 6. Took discipline



7. "Significant"



@gapingvoid





Accountability







Privacy

Kate Dewhirst

www.katedewhirst.com

kate@katedewhirst.com

Follow me on Twitter: @katedewhirst

Facebook: Kate Dewhirst Health Law

LinkedIn: Kate Dewhirst