



Canadian Mental  
Health Association  
Waterloo Wellington

Association canadienne  
pour la santé mentale  
Waterloo Wellington

# Privacy Culture Universities & Colleges

**Anna Tersigni Phelan**, Chief Privacy/Risk/HIM

**Meredith Gardiner**, *Director of Services, Regional*

**Brooke Young**, *Manager, Police Services and Mental Health & Justice*

# Agenda

1

- Privacy and Mental Health

2

- FIPPA

3

- PHIPA

4

- Common Privacy Issues

5

- Privacy Culture on Campus

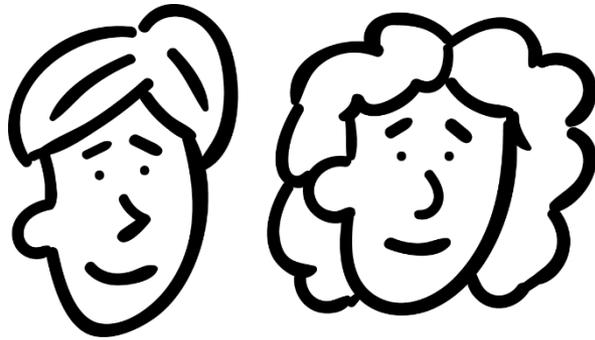
6

- Scenario & Questions

7

- Privacy References and Resources

# Why Does Privacy & Recorded Information About Us Matter?



It impacts our lives, hopes, and future.

# Privacy – Definition

- Influence of new media technologies further complicates meanings of privacy.
- Harvard Law Review (1890), defines privacy as the right ‘to be let alone’.
- People breach their own privacy by disclosing very personal information when using new media without considering negative consequences such as third parties gaining access to private information for bullying, marketing, scams, or identity theft.

# Why is it Critical to Protect Privacy?

The need to protect the privacy of individuals' Personal Health Information (PHI) has never been greater:

- extreme sensitivity of PHI
- greater number of individuals involved in the delivery of health care
- increased portability of PHI
- emphasis on information technology and electronic exchanges of PHI, and
- recorded information – is it accurate?

# Consequences of Inadequate Attention to Privacy

- discrimination, stigmatization, and psychological or economic harm
- individuals avoiding testing or treatment
- individuals withholding or falsifying information
- loss of trust or confidence in the health care system
- cost and time in dealing with privacy breaches
- legal liabilities and proceedings
- background checks by potential employers and harm to reputation

# Ontario Privacy Laws

- Ontario's Freedom of Information and Protection of Privacy Act (FIPPA) applies to over 300 provincial institutions such as ministries, provincial agencies, boards and commissions, as well as community colleges and universities.
- FIPPA was imposed on Ontario's campuses in 2006.
- The Provincial and Municipal Acts (MFIPPA) helps to protect our personal information held by provincial and local government institutions applies to over 1,200 municipal institutions such as municipalities, police services boards, school boards, conservation authorities, and transit commissions.
- Office of the Information and Privacy Commissioner of Ontario (IPC) ensures that public institutions abide by the Acts.
- Personal Health Information Protection Act, 2004 (PHIPA) governs the collection, use and disclosure of personal health information within the health-care system and also gives us the right to request access to our own personal health information held by HIC. PHIPA covers individuals and organizations in Ontario including hospitals, pharmacies, laboratories and health care providers such as doctors, dentists and nurses; community mental health, etc.

# What Does FIPPA Do?

- Provides the right to access information under the control of institutions with principles that:
  - information should be available to the public
  - necessary exemptions from right of access should be limited and specific, and
  - decisions on disclosure of government information should be reviewed independently of the government.
- Protects the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information (Ontario, FIPPA, 2010, s.1)
- Oversight Ontario Privacy Commissioner

# Personal Information (PI)

- **Recorded Information:** can be recorded in any format, such as paper records, electronic records, digital photographs, videos, or maps.
- **Identifiable Individual Information:** reveals something of a personal nature about the individual.
- It is reasonable to expect that an individual can be identified from the information (either alone or by combining it with other information).
- Examples include a person's name when combined with other information about them, such as their address, sex, age, education, or medical history.
- These examples are not exhaustive and many other kinds of information may still qualify as personal information.

# Personal Health Information Protection Act (PHIPA)

- PHIPA came into force November 1, 2004.
- Majority of PHIPA governs “personal health information” in the custody or control of:
  - “Health Information Custodians” or
  - “Agents” of Health Information Custodians.
- However, the Act also has broader application, for example, it contains restrictions on the use and disclosure of PHI by non-custodians that receive PHI from Custodians.

# Recent Amendments to PHIPA

Amendments to PHIPA proclaimed in force include:

- Privacy breaches meeting a threshold to be prescribed in regulation must be reported to Information Privacy Commissioner office.
- Privacy breaches must be reported by HIC to health regulatory colleges where a member of the College, who is employed, holds privileges or is affiliated with the HIC, has committed or is suspected of having committed a privacy breach.
- Fines have been doubled for offences from \$50,000 to \$100,000 for individual and \$250,000 to \$500,000 for organizations.
- The limitation period for prosecutions has been removed.

# Bill 119 – Highlights

- changed definition of “use” to include “view”
- added responsibility on HIC to ensure PHI not collected without authority (new s. 11.1)
- added responsibility to report privacy breaches to IPC (particulars to come in regulations)
- must tell affected individuals they have a right to complain to the IPC
- updated how a breach by researcher should be handled
- updated rules for Agents and responsibilities for HIC about Agents
- Bill 119 was passed on May 18, 2016, amending the Personal Health Information Protection Act (PHIPA) and the Quality of Care Information Protection Act (QCIPA)

<http://ddohealthlaw.com/app/uploads/2016/04/Proposed-Changes-to-PHIPA-through-Bill-119-Blacklined-Not-Official-Version-2016.pdf>

# Health Information Custodians (HIC)

Health Information Custodians (HIC) includes:

- a health care practitioner who provides health care
- a person who operates a group practices of health care practitioners who provide health care
- a hospital, psychiatric facility, and independent health facility
- a pharmacy, ambulance service, laboratory, or specimen collection center
- a long-term care home, care home for special care
- a community care access corporation
- a medical officer of health of a board of health
- Minister/Ministry of Health and Long-Term Care
- Canadian Blood Services

# What is Personal Health Information (PHI)?

Personal Health Information (PHI) is identifying information about an individual relating to their health and health care such as:

- clinical information
- family history
- health provider
- health card number

# Mixed Records

- Subject to certain exceptions, HIC that are also institutions within the meaning of public sector privacy and access to information legislation are governed by PHIPA, not FIPPA or MFIPPA, with respect to PHI in their custody or under their control.
- Identifying information about an individual that is not health-related but is contained in a record that includes PHI.
- All other recorded information that is not PHI and is in custody and control of an organization that is both a HIC and an institution or part of an institution is subject to FIPPA or MFIPPA as case may be.

# Sanctions for Unauthorized Access

- investigation by privacy oversight bodies
- prosecution for offences
- lawsuits
- discipline by regulatory colleges and investigations by other oversight bodies
- discipline by employers

# Agents

- An Agent, with the authorization of a HIC, acts for or on behalf of the Custodian in respect of personal health information.
- An Agent may include a person or company that contracts with, is employed by, or volunteers for a Custodian, and may have access to PHI.
- A HIC remains responsible for the PHI collected, used, disclosed, retained, or disposed of by an Agent.
- Duties imposed on Custodians and their Agents under the Act include:
  - collection, use, and disclosure of PHI
  - security of PHI
  - responding to requests for access to, and correction of, records of PHI, and
  - transparency of information practices.

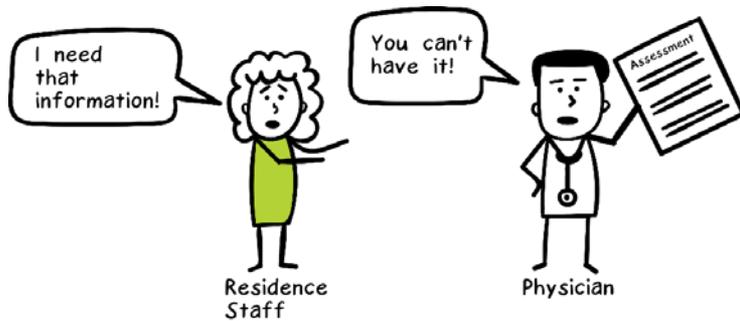
# Our Obligation as HIC

1. appoint a Privacy Officer
2. post information management practices (staff/clients/public)
3. have clear rules about privacy (usually in policy)
4. **ensure Agents are informed about their duties under PHIPA (training)**
5. respond to public inquiries
6. respond to requests for access/correction to a record of PHI
7. Privacy Impact Assessments for new technology
8. take reasonable steps to ensure accuracy of PHI
9. ensure protection of PHI against loss, theft, unauthorized access, use or disclosure, copying, modification, disposal (**and notify affected individuals if there has been a privacy breach; report to IPC regulations 2019 in force**)
10. ensure that records of PHI are retained, transferred, and disposed of in a secure manner

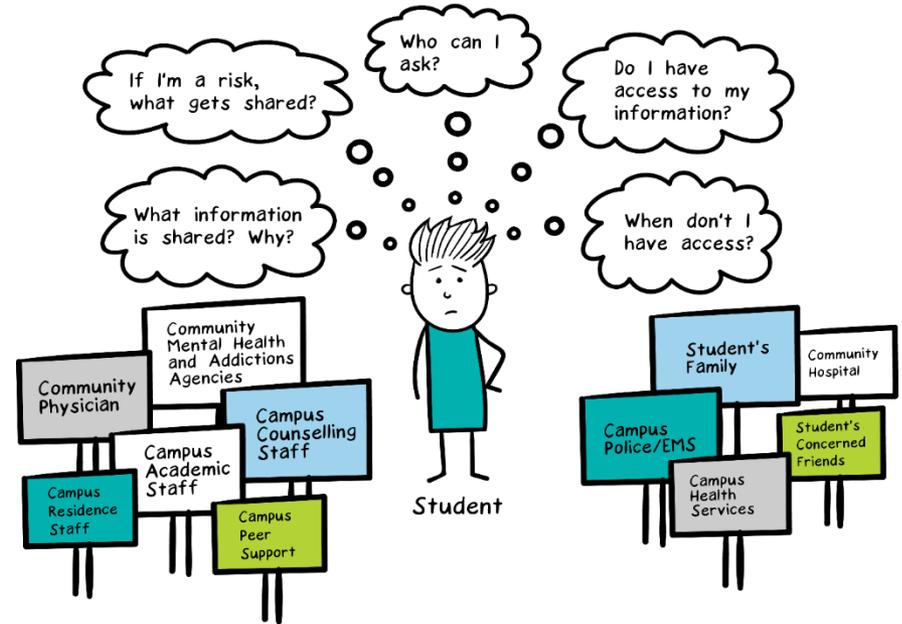
# Collection, Use, and Disclosure

- not permitted to collect, use, or disclose PHI if other information will serve the purpose more than reasonably necessary, unless:
  - the individual **consents**
  - permitted or required to be made without consent
- Providing PHI to an Agent is considered a use by the Custodian rather than a disclosure to the Agent.

# Common Privacy Dilemmas



Sharing Information



Multiple Stakeholders

# Consent and PHIPA

- Collection, Use and Disclosure (silent on access – think SDM)
  - Capacity test – not an age threshold
  - Persons who may consent
    - An individual who is capable (and if 16, a representative authorized in writing)
    - If child is under age of 16, a parent or CAS **UNLESS**
      - **Info about treatment child decided on own**
      - **Counseling under CFSA**
    - If incapable, the incapable person's substitute decision-maker
    - Estate trustee

# Table

AGE	CAPACITY	DECISION MAKER
Person of any age	If capable	Can make decisions about release of everything in his/her 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 his/her 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 his/her own BUT NOT IF THE CAPABLE CHILD OBJECTS TO PARENT MAKING SUCH DECISIONS

# Kids and PHIPA

- For an **incapable child**, the parents together make decisions about treatment and privacy
- If there is a separation or divorce – if you are going to only follow the instructions of one parent exclusively – you need papers to show one parent has “custody” and other has “access” or papers to show one parent is restricted from information about child

# Current Practices for Release of Information

- signed express consent
- verbal express consent
- implied consent with notice
- combination
- no consent



# Collaborative Care & Access to Personal Health Information

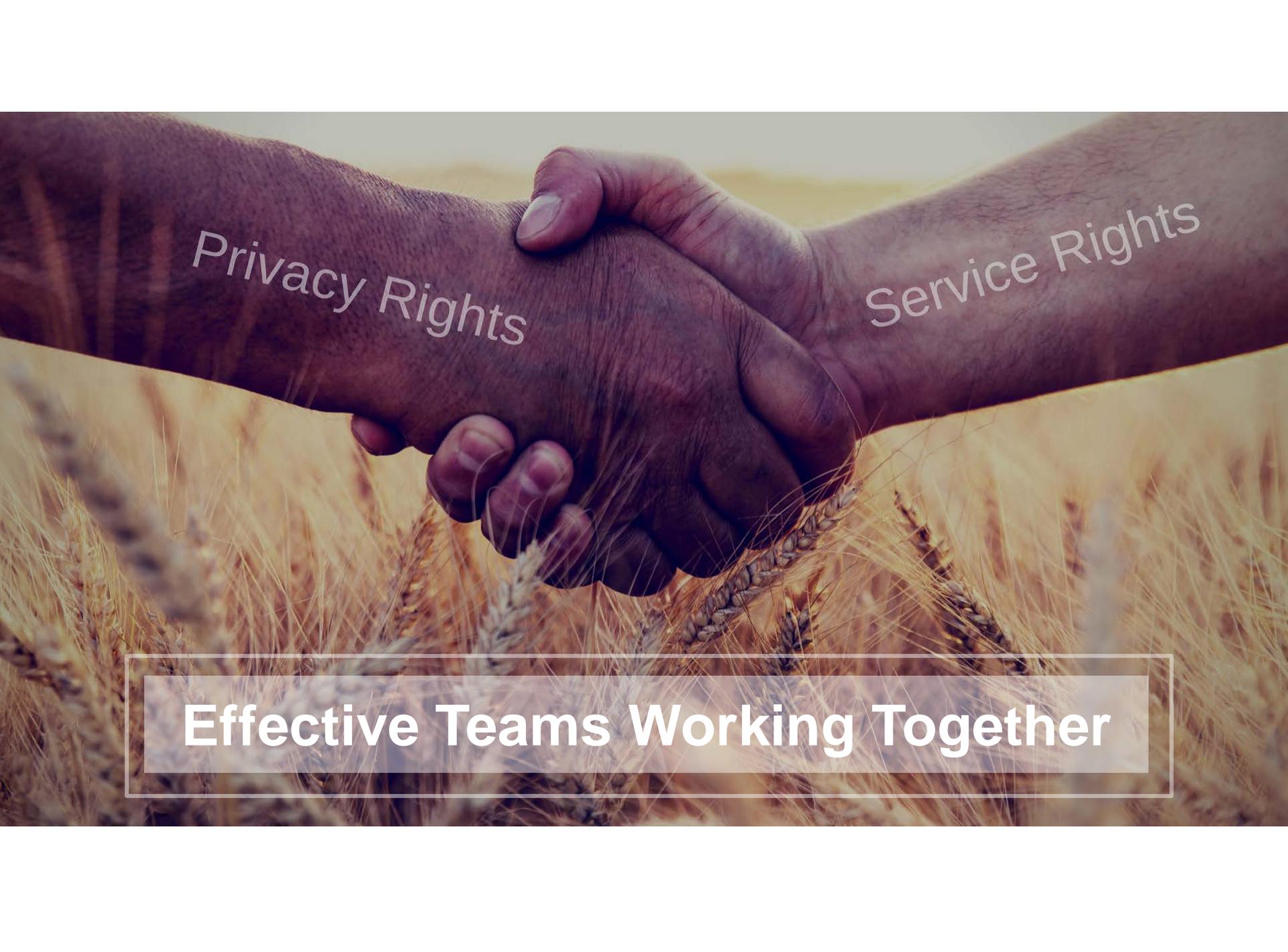
- PHIPA: clearly has no requirement for express consent in the context of providing care between HIC (IPC: 2008)
- can rely on implied consent if:
  - disclosing to a direct health care provider AND
  - for purpose of providing or assisting in providing health care

A hand is shown from the palm side, holding a black compass. The compass face is visible, showing cardinal and intercardinal directions (N, NE, E, SE, S, SW, W, NW) and degree markings. The background is a soft, out-of-focus sunset or sunrise over water, with warm orange and pink tones. A semi-transparent white rectangular box with a thin black border is centered over the hand and compass, containing the text.

**Need Consistent Circle of Care Approach**

# Shared Care Approach

- **Interprofessional Care:** all health professionals work together in developing a documented plan of care with an individual.
- **Interprofessional Person-Centered Collaborative Practice:** “a partnership between a team of health providers and a person where the individual retains control over his/her care and is provided access to the knowledge and skills of team members to arrive at a realistic team shared plan of care and access to the resources to achieve the plan” (Orchard 2007).

A close-up photograph of two hands shaking in a firm grip. The hands are positioned in the center of the frame, with the fingers interlocked. The background is a soft-focus field of golden wheat stalks, suggesting a natural and fruitful environment. The lighting is warm, creating a sense of positivity and partnership. The text 'Privacy Rights' is written in white, sans-serif font across the left hand, and 'Service Rights' is written in the same font across the right hand. At the bottom, a white rectangular box with a thin border contains the text 'Effective Teams Working Together' in a bold, white, sans-serif font.

Privacy Rights

Service Rights

**Effective Teams Working Together**

# Caution

18 (3): A consent to the disclosure of PHI about an individual must be express, and not implied, if:

- a HIC makes the disclosure to a person that is not a HIC,  
or
- a HIC makes the disclosure to another HIC and the disclosure is not for the purposes of providing health care or assisting in providing health care.

# Exceptions to Express Consent

- public interest/grave hazards
- disclosures to Public Health Authorities
- compassionate circumstances
- Ontario Society for the Prevention of Cruelty to Animals (SPCA)
- Child and Family Services Act
- Highway Traffic Act

*Need to know risk information is permitted to be shared to enable the provision of a healthcare intervention*

# Tension Between FIPPA & PHIPA On Campus

- FIPPA and PHIPA outline situations in which counsellors, professors, or campus security can disclose private personal and institutional information.
- tension between protection and disclosure
  - example: student who is psychologically vulnerable or if there is potential for violence on campus

# Risk Call

- Reasonable expectation of privacy by students.
- Both FIPPA & PHIPA specify that it is 'reasonable' to disclose private information in public interest.
- In extraordinary circumstances, it is in the public interest to name a minor in order to solve a crime, or to name a potentially dangerous, or emotionally 'at-risk' student on campus.

# Disclosure to Police

- Duty to Warn is triggered when there are reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons (PHIPA(40)(1); F&CS Act).
  - gives the ability to disclose PHI to reduce serious risk of harm
  - need to know PHI shared for purposes of health care
- There is no general legislative authority that requires HSP or citizens to report alleged criminal activity to the police with the exception of the Mandatory Gunshot Wounds Reporting Act, 2005.

# Sharing Information with Families

- practice family-centered care delivery
- need to ask individual who they want involved in their care, treatment, and information sharing
- can offer supportive information to families (even if individual does not want the family involved) such as links to resources
- can contact relative, friend, or SDM if the individual is injured, incapacitated, ill, or unable to give consent personally
- can contact family for the purpose of identifying a deceased individual

# How to Enable A Privacy Culture On Campus

*“The awareness that there is likely no ‘reasonable’ expectation of personal privacy in any space, private or public, is one of the strongest arguments for personal discretion.”*

*Canadian Journal of Communication: Martin R. Dowding, Assistant Professor  
– Wilfrid Laurier University, 2011*

# Students' Aware of Privacy Rights

- ✓ right of access his/her own health record
- ✓ right of file correction/addendum in 30 days
- ✓ right to have his/her “story” written with facts, unbiased, and not subjective
- ✓ right of to know what is being said, written about him/her, and to access log of all information about him/her that is released and why and to whom
- ✓ right to know if/when his/her information is breached
- ✓ right to be given IPC contact information for oversight
- ✓ Faculty/Agents are obligated to respect these rights and have signed Privacy Pledges to this effect
- ✓ process to manage third party requests; access to Privacy Officer if student has questions/concerns
- ✓ compliance necessary to apply Privacy Breach process if/when privacy breach occurs

# Students Aware of Their Rights to Lockbox

- A HIC may use PHI about an individual, for the purpose for which the information was collected and for all the functions reasonably necessary for carrying out the purpose, but not if the individual expressly instructs otherwise.
- Clients have a right to make choices about how their personal health information is used within the institution
- One way that clients can exercise this choice is to ask to use a “lockbox” to hide clinical information from health care providers within the HIC.

# What Are The Limits of a Lockbox?

A lockbox cannot be used to:

- Restrict information sharing with “non-health care providers” (such as family, employers, police, insurers) because those disclosures require express consent anyways.
- Prevent you from making mandatory disclosures to the courts or public authorities (such as CAS) because you are required by law to report.
- Limit legally permitted administrative uses for PHI (such as teaching, risk management, program planning, or funding purposes).

# Clinical Practice Impact

- You may be restricted from accessing information about your students.
- You may be asked not to share certain information with external health care providers.
- You may be asked not to share certain information with other clinicians/stakeholders within your organization.
- Someone has to be responsible to implement a lockbox (either technological or administrative).
- You must notify a receiving HIC if you are not sending all the relevant information/records because of a lockbox: “I am not authorized to disclose other relevant information”.

# Harmonized Privacy Policies and Procedures Needed

Harmonized privacy policies & procedures should address:

- privacy training
- privacy assurance (i.e. privacy readiness assessments)
- logging, auditing, and monitoring
- consent management
- privacy breach management
- privacy complaints and inquiries management
- access and correction

# Safeguards

- Must ensure that records of PHI are **retained**, **transferred**, and **disposed** of securely.
- Must take **reasonable steps** to ensure PHI is protected against:
  - theft, loss, and unauthorized use or disclosure
  - unauthorized copying, modification, or disposal
- Must **notify individuals** at the first reasonable opportunity if PHI is stolen, lost or used, or disclosed without authority.

# Transparency

- As Custodians we must **designate a contact person** responsible for compliance.
- We must make available a **written public statement** that describes the Custodian's information practices, including the **administrative, technical, and physical safeguards** in place.
- Written public statement must also include information about:
  - how to **contact** the Custodian
  - how individuals can **access or correct** their records
  - how individuals can **complain** to the Custodian and the IPC

# Detecting and Deterring Unauthorized Access

Reducing the impact of unauthorized access risk through:

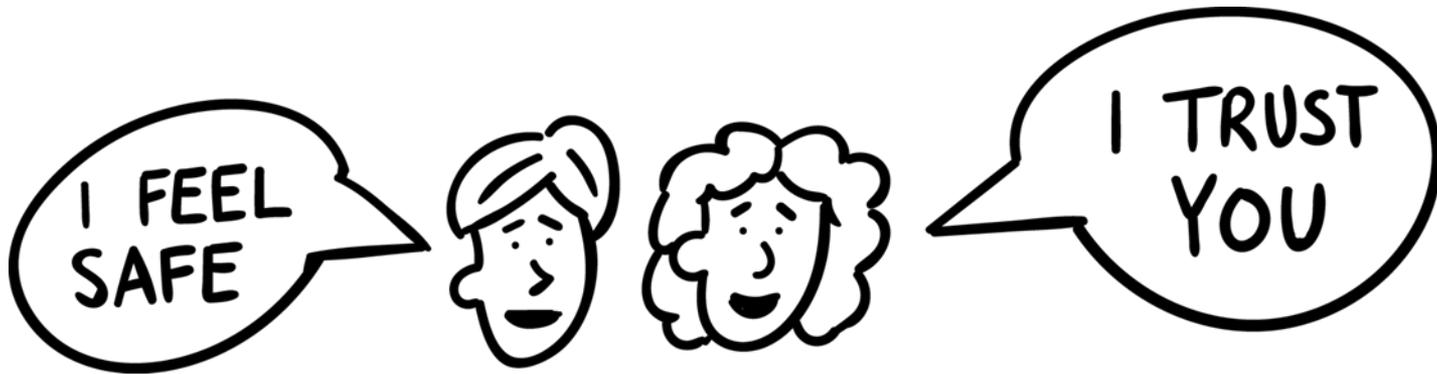
- ✓ policies and procedures
- ✓ training and awareness
- ✓ privacy notices and warning flags
- ✓ confidentiality and end-user agreements
- ✓ access management
- ✓ logging, auditing, and monitoring
- ✓ privacy breach management
- ✓ discipline



Detecting and Deterring  
Unauthorized Access to  
Personal Health Information



# Impact of Student Awareness of Privacy Protection Standards



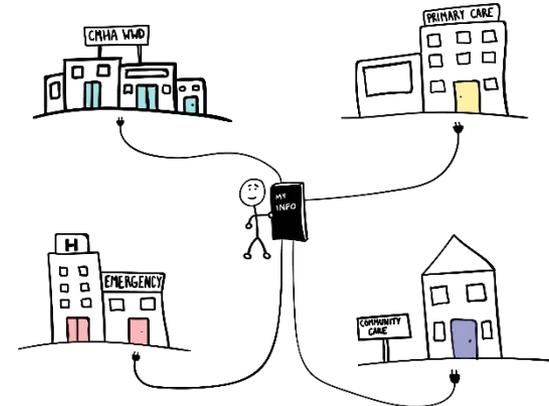
Trust + Safety = More people reach out for help

# Student Informed of Privacy Rights/Responsibilities

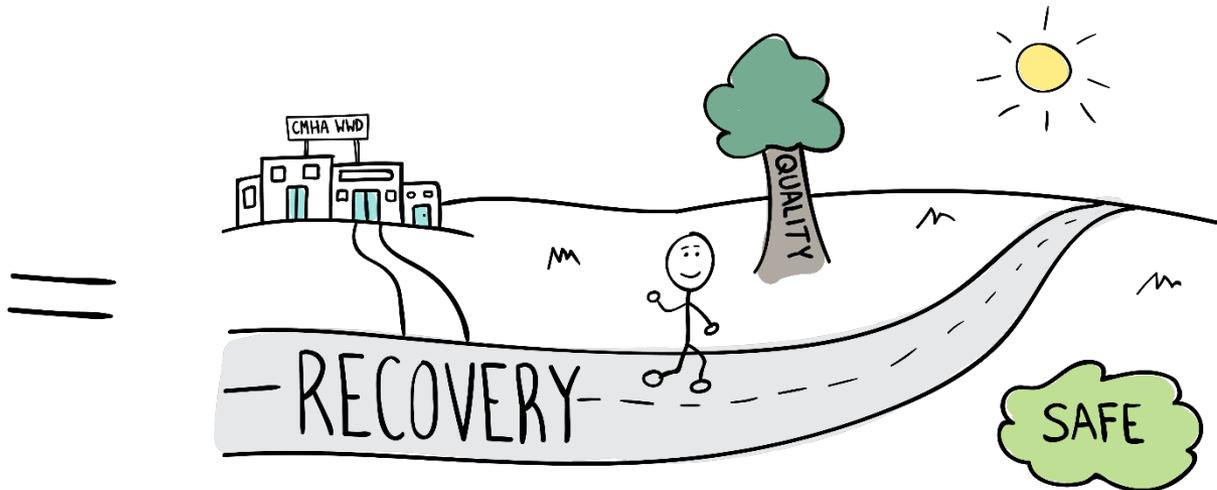


Integrated & Collaborative Care + My/Significant Other Participation

+



Accurate & Protected Information that Follows Me



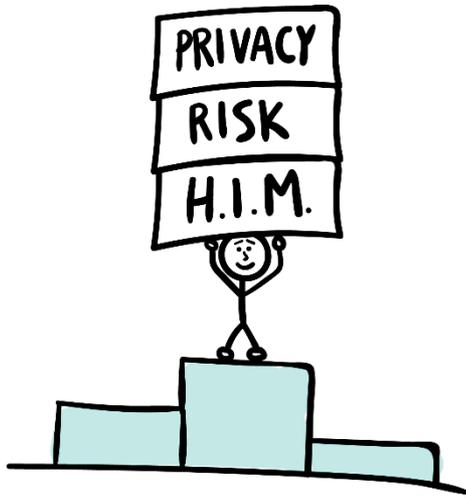
Safe, Quality Care on Campus

# Privacy as an Enabler in Partnership With Students

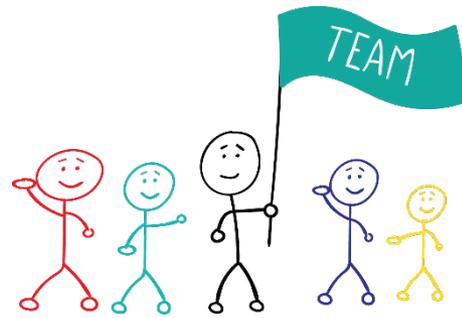
The following privacy rights are expected for each student served in this partnership:

- ✓ a culture of privacy + robust privacy program is in place on Campus
- ✓ Privacy Notice posted in agency, website, pamphlets
- ✓ faculty review/sign annual privacy pledges
- ✓ faculty trained – privacy practices – ongoing
- ✓ privacy policies/procedures are in operation and current
- ✓ regular privacy audits are conducted and logged
- ✓ DSA – provincial/federal initiatives for shared databases + ROI
- ✓ Privacy Breach Incident processes in place
- ✓ Right to Access/Correction/Block PHI easy to enact
- ✓ IPC – oversight – contact information available

# How Could We Do It?



Make it a priority!  
Invest in Privacy,  
Risk, and H.I.M.

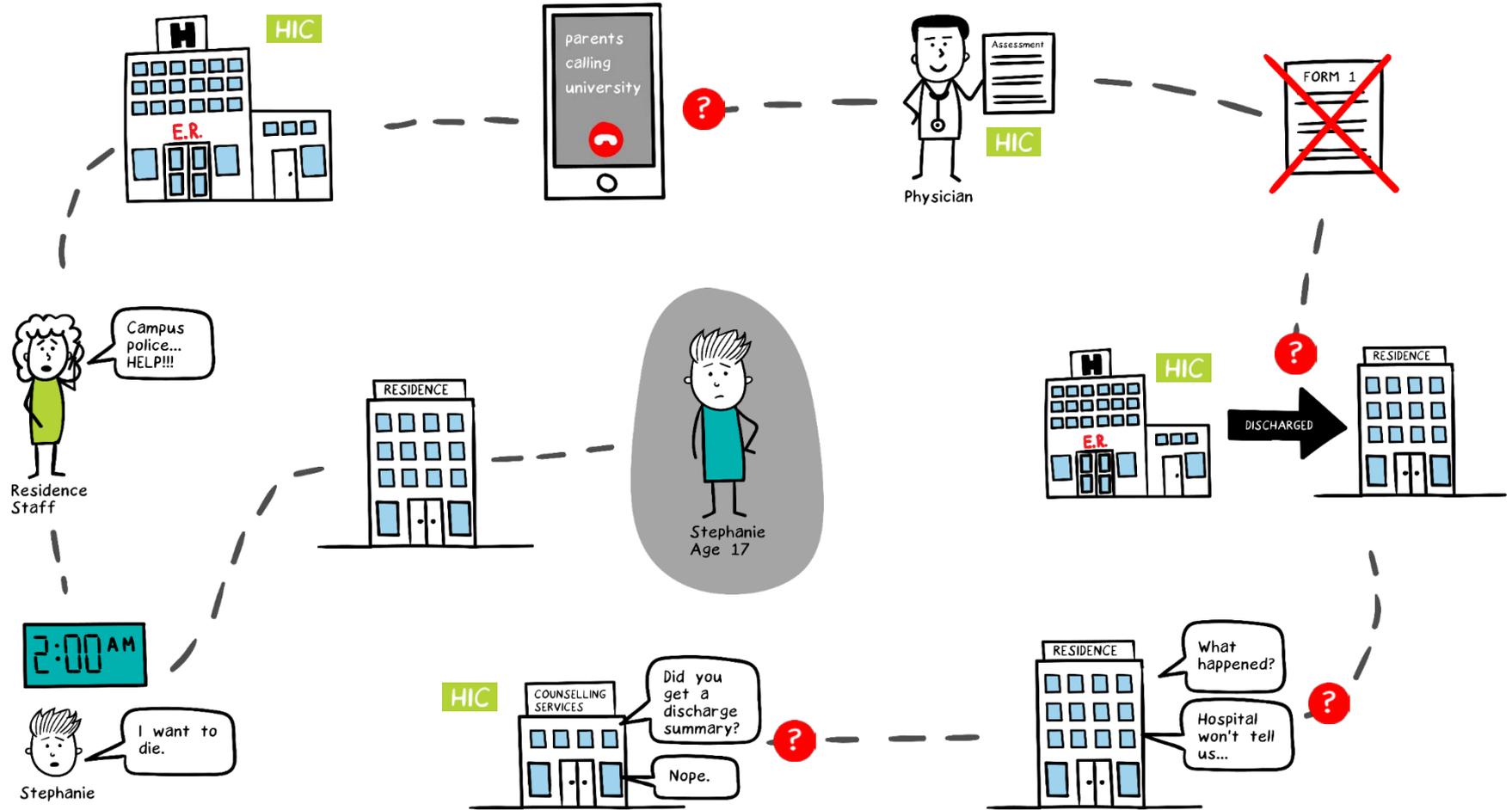


Work together  
and share  
resources.



Adopt + Use the  
same approach  
to lead in the  
education sector.

# Scenario



# Privacy Resources

- **Information and Privacy Commissioner of Ontario**
  - [45 Minute PHIPA Training Video](#) for all health sector staff
  - [PHIPA Fact Sheets](#)
  - [PHIPA Orders](#)
- **College of Physicians and Surgeons of Ontario**
  - [Confidentiality of Personal Health Information](#)
  - [Medical Records](#)
  - [Appropriate Use of Social Media by Physicians](#)
- **College of Nurses of Ontario**
  - [Confidentiality and Privacy – Personal Health Information](#)
  - [Social Media](#)

# References

- Practice Tool for Exercising Discretion: Emergency Disclosure of Personal Information by Universities, Colleges and Other Educational Institutions (Cavoukian & Loukidelis, 2008)
- CMHA Ontario Privacy toolkit: [www.privacytoolkit.ca](http://www.privacytoolkit.ca)
- Iacobucci: Police Encounters with People in Crisis (2014)
- Police + Mental Health – A critical review of Joint Police/Mental Health Collaborations in Ontario (2001)
- OACP Guideline for Police Record Checks (June/14)
- IPC Guide to the Personal Health Information Act
- OHA Practical Guide-Mental Health/The Law in Ontario
- IP HIC Working for Non-HIC
- Psychiatric Patient Advocate Office (Fact Sheets)