Privacy Training for Sir Sandford Fleming College of Applied Arts and Technology

Simmie Palter

Kathy O'Brien

February 26, 2020

Revised Agenda

FIPPA - Part 1 (1:05pm)

1. General Privacy Overview (10 minutes)
2. Personal Information Overview - Access Requests and Breach Process (40 minutes)
3. New 'Privacy Website' Presentation (Sarah Beirness and Dean Shamess) (5 minutes)

Questions and Answers (and Coffee) - 15 minutes

Break – 5 minutes

PHIPA - Part 2 (2:30pm)

***Only attendees who work with Personal Health information are required to stay for Part 2.*

- Personal Health Information Overview and Access Request Process (PHIPA) (40 minutes)

Questions and Answers - 15 minutes

DDO HEALTH LAW

FIPPA Privacy Overview

Freedom of Information and Protection of Privacy Act

Privacy Overview

- What is the difference between privacy and confidentiality?
  - Privacy of individuals
  - Confidentiality of an individual's information

- Where do privacy rules come from?
  - Federal/provincial/municipal law & regulations
  - IPC Guidelines and Directives
  - Orders and Reports of the IPC – provide guidance on interpreting the law

- Who oversees privacy matters in Ontario and Canada?

  Information and Privacy Commissioner of Ontario
  https://www.ipc.on.ca/
  Office of the Privacy Commissioner of Canada
  https://www.priv.gc.ca/en/

Privacy Overview (continued)

- Why is privacy important?
- Create a culture of privacy
  - We are all responsible;
  - We share Personal Information (PI) with other College employees only if necessary for our job duties;
  - We do not view records unless those records are directly related to our job duties;
  - We do not share PI outside of our job with anyone, for any reason; and
  - Ideally, we all sign confidentiality agreements
- Limit use of personal information
  - Use other information when necessary; use PI only if necessary for your job duties
  - Notify regarding purposes of collection and use; seek and obtain consent; give option to withdraw
- Provide a contact person (Freedom of Information (FOI) Coordinator)
  - Person who advises on access to information and protection of privacy for the College
  - Important to identify one individual as the contact person
- Conduct random audits employee & contractor use of College systems

DDO HEALTH LAW

Freedom of Information and Protection of Privacy Act (FIPPA) Overview

- Applies to institutions (180) – ministries, agencies, hospitals, universities, colleges
- Head – Chair of College's Board of Governors
- Requires government and quasi-government institutions to:
  - have legal authority to collect personal information and tell you that authority at the time of collection
  - preserve access to records relating to the institution's business
  - facilitate access to records according to these principles:
    - Information should be publicly available
    - Exemptions should be limited and specific
    - Disclosure decisions are reviewed independently (by the IPC)
- Encourages transparency in government and quasi-government operations
- Applies to records created or received by the College and that relate to the College's mandate

Personal Information Overview - Access Requests and Breach Process

What is Personal Information as defined by FIPPA? - *Who "owns" it?*

- What is personal information (PI)?
  - About an identifiable individual; reveals something personal
  - Student PI
  - Employee
  - Examples of PI (see next slide)

- What is not Personal information
  - Business contact information
  - Addresses or names alone
  - Business confidential information

- Who owns Personal Information? The person it relates to. Under FIPPA, when an individual asks for access to their PI under FIPPA, they are asking for the College's records of PI.

DDO HEALTH LAW

Personal Information – *What is PI and what is not PI?*

- age, race, ethnic or national origin, religion, colour, gender, sexual orientation, family/marital status
- medical, psychological, education, criminal, employment history or financial transactions of individual
- fingerprints, blood type, OHIP#, SIN
- identifying number assigned to the individual
- private correspondence sent to the College and replies that would reveal the contents of the original correspondence

Personal information does not include:

- the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity;
- information about an individual who has been dead for more than thirty years; and,
- records of graduation that are otherwise publicly disclosed.

DDO HEALTH LAW

Personal Information - *What is PI and what is not PI?*

- A name, by itself, is not PI by definition. A name is PI when it appears with other personal information relating to an individual or where the disclosure of the name would reveal other personal information about the individual.

- For employees the information must be about the employee in a personal capacity to be considered PI. As a general rule, information associated with an individual in a professional, official or business capacity will not be considered to be "about" the individual unless it reveals something of a personal nature.

- The context in which the information appears is important. It is important to examine the context in which information appears to determine whether it constitutes PI or not. Depending on the context, information may not meet the definition of personal information because it is, for example, information about an individual in a business capacity.

DDO HEALTH LAW

Personal Information – Respecting Employee Privacy

- All personal information kept by the College should be accurate and up to date
- Some employee information (in College records) is included under FIPPA, and could be requested, including:
  - employment contract
  - position, title, salary (disclosure may be required by law, such as for the Sunshine List)
  - employee expense records
- Some records are excluded from FIPPA, such as certain types of labour relations records (in which the College has an interest) and negotiations between an employee and the College (s. 65), however, the College still has discretion under FIPPA to disclose excluded records
- As seen earlier, in the definition of PI, certain employee information is not considered PI:
  - e.g. name, position, contact information.
  - Generally information associated with an individual in a professional, official or business capacity will not be considered to be "about" the individual unless it reveals something of a personal nature.
  - Context is key – even if information in the record = PI, it may be subject to exemption or exclusion

DDO HEALTH LAW

FIPPA – Collecting Information

- Collect only for the following purposes:
  - Administration of college
  - Purpose authorized by law
  - For law enforcement

- Must notify of collection and authority for collection and purpose(s):
  - "The information you provide on this form is collected by the College under the authority of the *FIPPA and the CAATA and is used by the College to plan and provide College programs, to process admissions and registrations, to conduct administrative activities related to the above and for purposes consistent with the above purposes.*"

- Must seek new consent for previously unidentified purpose

DDO HEALTH LAW

FIPPA – Indirect Collection

Collect directly from the individual to whom the information relates unless:

- Individual permits another method of collection (should be express and written)
- Individual expressly permits the College to receive the information
- The law permits the information to be disclosed to the College without the individual's consent
- The information is needed for law enforcement
- The information is collected to conduct a legal proceeding or possible proceeding (court or tribunal)
- Information is collected to determine suitability for an honour or an award to recognize outstanding achievement or distinguished service
- Information is in a credit report

FIPPA – Records

- Records
  - General (must relate to the activities and operations of the College – i.e. fiscal, legal, support decision-making)
  - Personal information

Examples:

  - working drafts
  - voice messages, written records, maps, text messages, meeting minutes, diagrams, reports, photos, drawings on a napkin, handwritten notes, final documents
  - includes records that are held in an electronic database but are producible, provided that production does not interfere with normal business operations of the College:

- Records vs. Personal Information
  - Personal information belongs to the individual to whom it relates
  - Records belong to the institution creating or receiving them, in most cases

FIPPA – Excluded Records

Section 65

- Some types of records are excluded from the ambit of FIPPA, for example:
  - Negotiations between the College and an employee
  - Meetings or discussions about labour relations in which the College has an interest
  - Several categories (beyond scope of this presentation)

- However, these records can still be disclosed at the discretion of the College

- To understand more about excluded records, see: https://www.ontario.ca/document/freedom-information-and-protection-privacy-manual

DDO HEALTH LAW

FIPPA – Using Personal Information

- Use must be for identified purpose
- Purposes are identified in the notice of collection/privacy policy/privacy procedures
- Use can also be for a purpose that is consistent with one or more of the identified purposes
- Identified Purposes include:
  - Providing College programs or services
  - Planning College programs or services
  - Determining suitability for admission and registration
  - Administrative purposes related to the above purposes
- Disclosure between employees of College = use
- Department Heads:
  - Limit Use to those employees & agents who need the information to provide services
  - Make reasonable efforts to prevent unauthorized disclosure and inadvertent destruction of, or damage to, Personal Information

FIPPA – Protecting and Preserving records

- College has legal duty to preserve records
- Records should be organized and retrievable (record retention schedule)
- College has duty to preserve personal information for access purposes – one year after use for records of PI unless subject of PI consents to earlier disposal (s.40(1); Reg. 460 s. 5)
- Protect Records: Technical, Administrative and Physical Safeguards
- Record disposal and destruction schedule

DDO HEALTH LAW

Record Retention and Destruction

- Protect personal information held by government and quasi-government institutions

- Safeguards:
  - Technological – firewalls, passwords, encryption, limiting user access, screen savers, daily backup, audit trail capabilities, secure VPNs (virtual private networks)

  - Administrative – privacy training, policies and procedures, confidentiality agreements, employee discipline, keep attendance lists private; contracts with ISPs, data hosts, audit, log of access, and record of breaches

  - Physical - clean desk policies, locked drawers and filing cabinets, keycard access to rooms where PI or PI systems are used or stored

DDO HEALTH LAW

FIPPA – Record Retention and Destruction

- Records of Personal Information must be retained for at least one year
- Destruction method must ensure records cannot be reconstructed
- Department Heads are responsible for creating, operationalizing and maintaining their own process for record retention and disposal, within the framework provided by FIPPA
- If the Record is in electronic format, the Personal Information must be adequately deleted so that it cannot be retrieved or reconstructed.
- The department must log the date and type of Record that was destroyed, or disposed of, how, and by whom.
- Certificates of Destruction may be requested from third-parties, and if requested must be identified by request date in the log.

DDO HEALTH LAW

FIPPA – Disclosing Personal Information to Third Parties

May Disclose:

- for identified purpose or consistent purpose
- disclosure to third party was implied in the identified purpose
- if the individual consents to the disclosure and identified the PI to be disclosed, the recipient's identity and the date of the consent
- to consultant or agent in order to perform duties on behalf of College – confidentiality and security contracts to be signed with consultant/agent
- required by law
- requested by law enforcement (pursuant to warrant or court order)
- risk of serious bodily harm to an individual
- compelling circumstances involving an individual's health or safety
- for compassionate reasons: individual is ill, injured or deceased and disclosure is to facilitate contact with close relative or friend
- to union rep, M.P. or M.P.P. but only with consent from the individual

FIPPA – Requests for Access – *Informal vs. formal*

- Informal vs. formal request for information
  - Informal includes: routine disclosure for certain repeat requests (e.g. requester's own transcripts and proactive disclosure)
- Requests for own information vs. requests for personal information

- Formal request under FIPPA (access request form)
  - Fleming College FIPPA Access Request Form complete and sent to FOI Coordinator
  - $5 fee applies

- General Principles of Access
  - Information to be available to the public
  - Exemptions and exclusions to be limited and specific
  - Disclosure decisions to be reviewed by independent third party (IPC)

FIPPA: Formal Requests for Access – *FOI Coordinator*

- Preliminary matters
  - formal vs. informal - written? Under FIPPA? Detailed? Includes the fee?
  - forward? transfer?
  - frivolous & vexatious?
  - Does the request ask for a record?
  - Does the request for PI identify the personal information bank or where the record can be found?
  - Is the record in the College's custody or control?
    - Custody = physical possession
    - Control = ability to make a decision about the record's storage or retrieval

- Circulate parameters of request to appropriate department head:
  - Keep third party requester's name confidential; can disclose category of requester but not if it will hinder access (e.g. lawyer or journalist)
  - Ensure records are identified enough to be searchable
  - Example (next slide)

FIPPA: Formal Requests for Access - *Example of internal communication*

- Formal FIPPA request for information is received by Privacy Coordinator
- Email sent from Privacy Coordinator to Department Head

****

Date: March 24, 2019

Please search your department for records that are responsive to the following request:

> *"all correspondence between the Registrar and Jodi Dimple between March 1, 2018 up to and including December 31, 2018"*

Please forward any responsive records to my attention by March 31, 2019.

Directory of Records (maintained by the Ontario government)

- Head responsible for providing this information to the Ministry of Government and Consumer Services (Ontario)

- Academic (2667), Finance and Facilities (2668) , IT Services (2669), Learning Resource Centre (2689), Student Services and Registrar's Office (2701), Human & Organizational Development (2747), Board of Governors (2746), President's Office (2748)

- https://data.ontario.ca/dataset/directory-of-records-under-the-freedom-of-information-and-protection-of-privacy-act/resource/59a2f906-5f14-4375-80fc-477362d3307b

- Directory of Institutions
  - https://www.ontario.ca/page/directory-institutions

FIPPA Requests for Access – *The search for records by the Department(s)*

- Search must be reasonable
- No need to search if experienced employee (i.e. experienced with record or program) can explain why the record does not exist
- Reasonable search:
  - uses information in the request
  - is conducted by personnel who are knowledgeable about the content and the location of the records
  - personnel consult with others when necessary to locate the records
  - department head ensures data regarding search for records is documented
    - record details of dates, directories, amount of time spent and types of files searched to locate the records
  - respect time limits when responding to search request
- Time limits: all FIPPA access requests to be responded to within 30 days, unless extended
- Once Disclosed: no limits on use

DDO HEALTH LAW

FIPPA Exemptions - *Mandatory and Discretionary*

- Long list of reasons for exempting material from disclosure (Head decides, unless delegated to someone else)
- Some exemptions require withholding (Cabinet records, third party procurement or commercial information; PI about individuals other than the requester)
- Some exemptions are discretionary – so Head can decide to disclose or to withhold (on a case by case basis)
- General exemption for records that contain personal information disclosure of which would be an unjustified invasion of privacy (s. 21 FIPPA)
- Department Heads, after searching for and identifying responsive records, can consider whether exemptions apply and recommend exemption in consultation with the Privacy Officer
- Department Heads consult FOIPP Manual available at https://www.ontario.ca/document/freedom-information-and-protection-privacy-manual (chapter 5)

DDO HEALTH LAW

FIPPA - Discretionary Exemptions

The College has discretion to decide to withhold certain records, or parts of records, when access to them is requested, subject to limitations found within FIPPA (s. 12 - 22). Some exemptions include:

- Advice or Recommendations – s. 13
  - to aid College in decision-making, but does not include factual material and other information
- Law Enforcement – s.14
  - When disclosure could interfere with an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.
- Economic Interests or Competitive Position of the College - s.18
  - When disclosure could harm the competitive position of the College – for example, disclosure of exam questions or testing procedures (when not re-using exam questions)
- Closed Meetings – s.18.1(1)
  - Substance of deliberations of a meeting of the governing body or a committee of the governing body of an educational institution if a statute authorizes holding the meeting in the absence of the public and the subject-matter of the meeting is a draft of a by-law, resolution or legislation; or is litigation or possible litigation.
- Discretion to withhold is exercised by the College; Department Heads to be alive to possible exemptions and discuss with FOI Coordinator

DDO HEALTH LAW

Requests (FIPPA) for access to third party commercial information

- See exemption (s. 17, mandatory)
- Contracts to be disclosed
- Procurement (tendering documents must contain FIPPA clause)
- Must notify third parties of request for disclosure and give third party 20 days to submit written reasons against disclosure; College decides about disclosure
- Third party not entitled to know identity of requester
- To be protected third party information must be
  1. Trade secret, scientific, commercial, financial or related to labour relations; and
  2. Supplied to the College in confidence; and
  3. Disclosure of the information could reasonably be expected to result in one of these 3 harms
     1. Harms that significantly prejudice the College's competitive position or interferes with contractual or other negotiations of a person
     2. Similar information no longer being supplied to the College and it is in the public interest that such supply continue; or
     3. Undue loss or gain to any person.

FIPPA – Requests for Access to Requester's Personal Information

- Requester has right to examine or have copies of his or her own personal information held by the College
- College to facilitate that access unless:
  - disclosure = unjustified invasion of another individual's personal privacy;
  - disclosure could reasonably be expected to seriously threaten safety or health of an individual
  - disclosure would reveal advice (policy options, possible courses of action) or recommendations (suggested course(s) of action to be accepted or rejected by the College) made by employee or contractor of the College (does not include facts, final reports, studies) – unless Head has publicly released the material
  - Information relates to law enforcement or to an employment related investigation that leads to discipline by College
  - College's commercial information that has monetary value if disclosed (e.g. trade secrets, commercial, financial, scientific or technical information)
  - Disclosure would prejudice economic interests or competitive position of the College. – e.g. exam questions and testing procedures may be withheld (unless those questions are re-used) if disclosure could reasonably be expected to prejudice the use or results of the tests or testing procedures.

Exemptions from Disclosure of own PI to Requester

- If the information is supplied in confidence and is evaluative or opinion material compiled solely for the purpose of:
  - assessing the research of a College employee or contractor
  - determining suitability, eligibility or qualifications for admission to the College, or
  - determining suitability for an honour or award to recognize outstanding achievement or distinguished service
- Research, which, if disclosed, would deny a specified researcher priority of publication where an intention to publish is clear (does not apply to raw data)
- If disclosure would be an offence under an Act. e.g. under the *Youth Criminal Justice Act* it is an offence to knowingly disclose certain court, police and government records relating to young offenders
- other exemptions are in the legislation (cannot review all – limited time)
- Practical example: If Student requests "blanket" consent for parents to access all of their PI held by the College – do not grant. Always be wary of blanket requests. Scope of disclosure should always be limited.

Providing Access

College must verify identity of requester before providing access

- Always ask for photo identification (but not a health card)
- Keep record of type of verification viewed, for audit (included on FIPPA form)

College keeps its own records and either grants access to the requester, to view, or makes copies for the requester.

FIPPA – Requests for Disclosure of Records of Someone Else's Personal Information

- Disclosure to someone other than the person to whom the personal information relates
  - placement employers
  - insurance companies – send to FOI Coordinator
  - lawyers - send to FOI Coordinator
  - parents

Need Written Consent to Disclose (consent should specify) :

- the Personal Information to be disclosed,
- the entity to whom the Personal Information is to be disclosed; and.
- the date, and duration, of the consent.

► See example, next slide

FIPPA – Requests for Disclosure of Records of Someone Else's Personal Information

- Example: Lawyer seeks client's own personal information and sends signed consent
  - Ensure scope of request; review date of consent
  - Can contact student and ask for new consent, if necessary
  - Lawyer sought former student's record of progress at the college; consent was outdated by more than 90 days; student asked to sign new consent; scope of request was too broad to identify responsive records; lawyer was asked to narrow the scope of the request

More Examples – Request for Disclosure of Someone Else's PI

- Parent asks about son or daughter's attendance at College, approval for student loan, copy of timetable, or other PI of student living at home with parent or elsewhere – no disclosure without student's written consent

- Local newspaper seeks a current student's enrolment status, in response to police investigation - no disclosure without student's written consent

- But College can disclose within the College to facilitate an internal investigation of possible offence (or to determine if an investigation is needed)

- Student logs written complaint to College about another student without that student's name and asks College for photo of student to append to complaint. No disclosure of photo without written consent.

Disclosure to Police

- Staff will not interfere with or obstruct a police officer in the exercise of his or her duties. Although there is no general legal requirement to assist police, staff will not deceive, mislead, or hinder the police
- Requesting a warrant or court order prior to disclosure of PI does not constitute hindering, interfering with or obstructing a police officer, unless the College is required by law to produce the information requested.
- Usually need subpoena, warrant or court order, scope of which must be carefully reviewed before disclosing (described in next slide)
- No fishing or fact-finding expeditions
- Disclosure should accord with Fleming policy
- Example: Police seek a particular student's timetable, as part of an ongoing police investigation about the student, without a warrant –no disclosure of timetable without a warrant [FIPPA s. 42(1)(g)]

Disclosure to Police (continued)

- Warrant: An official document, signed by a judge or a justice of the peace, commanding police to perform specified acts. e.g. search warrants, arrest warrants, Coroner's warrants.

- Subpoena or Summons to Witness: A legal document that compels a named individual to attend a court of law or other proceeding to answer questions or to produce documents or things.

- Court Order: A legal document issued by a court that compels a named person to perform specified acts, which may include producing documents or things; court orders may also prohibit actions.

Open-ended questions from Police

- Police arrive without any specifics about the person of interest and ask open ended questions – do not answer without prior consent or a warrant
- If staff believe that a student may fit the police description, staff should feel comfortable asking the police officer to wait while (discreetly – without automatically signally that the student is present) trying to obtain the student's consent to speak to the police. The police officer should also be encouraged to provide more context and detail with respect to their line of questioning to assist staff in obtaining consent. The student may wish to consult with a lawyer before speaking with the police. Staff must not be seen to advise a student that they "have to talk with the police".
- In the event that staff cannot obtain consent (student refuses or is incapable) and are unsure if the details provided by the police permit disclosure of any student information, staff should feel comfortable to tell police that they cannot disclose any information directly, and should direct police to the FOI Coordinator

DDO HEALTH LAW

Police Requests to Interview College Staff

- All police requests for statements or interviews with staff must be referred to and reviewed with the FOI Coordinator
- Staff will only share PI in a written statement or during an interview with student consent or in compliance with a warrant. Staff can ask police to arrange an appointment for a written statement or interview. College may support staff who choose to be interviewed.
- Staff may receive a summons or subpoena to testify in court. Such requests should be reviewed by the FOI Coordinator or a lawyer.
- If a police officer requests staff personal information, name, date of birth and work address and phone number are all that is required. Personal contact information does not have to be given. The officer's name, badge number, incident number and the circumstances must be documented.

Privacy Breach – *"what is it?"*

"Privacy Breach" covers every instance of theft, loss, and collection, use, retention, disclosure or destruction of PI that is not consistent with privacy law, whether intentional or in error. Some examples of privacy breaches include:

- Loss or theft of portable devices containing PI;
- Misdirected faxes or e-mails containing PI;
- Cyberattacks, including ransomware attacks on records of PI; and
- Deliberate unauthorized access to Records under the Custody or Control of the College, by a member of the College Community or others.

Privacy Breach – *"who is responsible?"*

Everyone is responsible for ensuring the security and confidentiality of PI under the Custody or Control of the College.

College Department Head(s) are responsible for:

- Responding to inquiries from the College Community related to concerns about PI and/or suspected breaches for their respective department(s);
- Notifying the Privacy Officer of all Privacy Breaches and suspected Privacy Breaches within their Department;
- Working with staff in their own Department(s) to follow the steps in the College's privacy breach procedure to enable timely reporting to the Privacy Officer;
- Ensuring Department staff are trained on and comply with this and all required procedures; and
- Containing Privacy Breaches and mitigating against future Privacy Breaches.

DDO HEALTH LAW

Privacy Breach – *"who is responsible?"…continued*

The FOI Coordinator is responsible for:

- Maintaining a record of all confirmed College Privacy Breaches;
- Working with Department Head(s) to assist with responses to internal PI inquiries and concerns;
- Providing formal notification to individuals affected by a confirmed Privacy Breach;
- Consulting with other Departments, senior management or legal counsel, as may be necessary;
- Notifying the IPC of confirmed Privacy Breaches, where required; and
- Reporting Privacy Breach statistics to the IPC annually.

Privacy Breach – *"who is responsible?"…continued*

Suspect a Breach? The 1st Step is Notification!

- Immediately upon learning of the privacy breach, employees should notify their direct supervisor(s) who in turn shall notify the applicable Department Head(s). The Department Head(s) will notify the FOI Coordinator.
- Ensure your Employees know they are not to initiate investigation of the breach unless specifically asked to do so by their Department Head(s).
- Depending upon the nature and seriousness of the breach, the Department Head(s), together with the FOI Coordinator, shall involve Senior Management and the President.
- The Department Head(s) is/are responsible for notifying the College FOI Coordinator as soon as reasonably possible after discovering or being notified of the breach.

NOTE: The College's new Operating Procedure "Privacy Breach Procedure" outlines all steps for when a suspected or confirmed privacy breach occurs!

DDO HEALTH LAW

PHIPA

PHIPA Overview and Access Request Process

Personal Health Information Protection Act, 2004

- Purpose:
  - Protect patient personal health information
    - collected, used, and disclosed by Health Information Custodians
    - in the course of providing health care for a health related purpose
  - Provide right of access by individuals to their PHI held by the custodian
  - Provide right of correction of that PHI, with limited exceptions

- Intent: Facilitate the provision of health care while protecting personal health information and facilitating access to that information

PHIPA Overview (continued)

Health information custodians at the College:

- Massage Clinic
- Counselling Services
- Health Services

Anyone employed or engaged by any of the above =“**agent of custodian**”

Agents use patient personal health information for custodian’s purposes, not for his or her own purposes.

Everyone working to provide or assist in the provision of health care at the College is responsible to protect personal health information provided by patients or clients of the services.

DDO HEALTH LAW

What is personal health information?

"**Identifying information**", oral or recorded, relating to:

- medical or health history
- information related to providing health care
- fact that person is a patient of nurse X
- health card number (no collection unless needed)
- X-rays, consultation letters, e-mail and voicemail messages
- conversations
- posted patient schedules
- donation of body parts or substances
- payment for health care services or eligibility for coverage (by OHIP or private insurer, for example)

"**identifying information**" is information that can be used alone or with other information to identify the individual

PHI is information that is collected, used and disclosed in the course of custodians providing health care to an individual.

What is NOT personal health information?

- PHI is NOT identifying information in a record in a Custodian's custody or control that relates to the Custodian's employees or agents and is kept primarily for a reason other than the provision of health care

- Examples:
  1. Information in the College's Human Resources records that relates to a College employee who has a medical disability and requires accommodation (not PHI)

  2. Information kept about a student or faculty member's attendance on campus for esthetic services or athletic coaching or personal training (not PHI)

  3. Immunization records kept in College records other than those relating to the provision of health care to the student (not PHI)

DDO HEALTH LAW

Personal Health Information Protection (PHIPA) and FIPPA

- FIPPA does not apply to personal health information held by a health information custodian. The College is a custodian in respect of the services identified.
- PHIPA does not limit a person's right of access under FIPPA as long as all PHI is reasonably severed from the record
- College can disclose a record under FIPPA but must remove the PHI from the record before disclosing it, BUT this does not make sense for an individual seeking his or her own PHI from the College.
- If requester wants own personal information related to his or her receipt of health care from a College health care services, the request must be made under PHIPA. Can clarify with requester before or after request is made – clarify intent and scope of the request. May need to revise request.
- Need consent for disclosure (use PHIPA Access/Correction Request form).
- Seek own PHI related to health care from the College, under PHIPA. (PHIPA Decision 17)

PHIPA – Sharing Personal Health Information – Circle of Care

- Can share patient personal health information to provide health care
- Consent of patient is implied for this purpose
- Intent of legislation is to facilitate provision of health care among custodians

Ask yourself this question:

Would it be reasonable for me to expect my nurse to tell _____ that I have cancer without my consent?

a) My oncologist (cancer specialist)? - custodian

b) My psychologist? – a custodian

c) The Canadian Cancer Society – not a custodian

d) Ontario Psychological Association – not a custodian

DDO HEALTH LAW

PHIPA Legal Requirements

- custodians must keep patient information confidential and secure
- all staff are responsible to keep patient information confidential
- no snooping
- only use patient information to help with providing health care to the patient
- only view or use patient information if you need it to do your job
- need consent to collect, use or disclose patient's personal health information
- capacity to consent; otherwise substitute decision-maker gives consent
- need to notify patients about purposes of collection for consent to be meaningful; patients may withdraw consent at any time
- patients own their PHI and have a right to access it and request correction of it
- if patients have questions about privacy, one person in the office should be the designated contact person or refer to the College privacy officer
- patients have a right to ask questions about the College's privacy policies and to complain about them to the College or elsewhere

DDO HEALTH LAW

NO Snooping

- Use includes viewing records on an electronic system
- Only view records you need to see to provide health care or to assist with provision of health care (i.e. to do your job)
- Cannot view family members' records
- Only view records to provide health care
- Penalties for snooping
  - Fines - up to $100,000 under PHIPA; prosecuted only with AG consent
  - Student fined $25,000 for snooping during placement
  - Creation of new laws in Ontario in last 8 years recognizing different kinds of invasions of privacy

PHIPA (lockbox)

- Patients can limit the amount of PHI that their health care providers are allowed to share
- If patient asks, must limit and make a note of limit in the patient record
- This may compromise the care that a patient can receive and must advise patient about this
- Specific rules regarding mental health records under the *Mental Health Act* (not within the scope of our discussion)

PHIPA snooping cases

- 2017-Ontario social work student at family health team snooped on hundreds of patients for a six month time period; fined $25,000
- Toronto Hospital: former maternity ward nurse and former RESP broker sentenced in June 2016 by Ontario criminal court to 3 months' house arrest, 2 years' probation and 340 hours of community service for inappropriate selling and using new mothers' contact information without consent

Disclosing PHI without consent

- disclosure is permitted if necessary to reduce or eliminate a significant risk of serious bodily harm to a person or group of people
  - Example: College staff suspects student at significant risk of suicide or harming others
- can disclose to police with or without a warrant s. 43(1)(g) – but rarely rely upon this, disclosing only a witness statement or report where a crime is suspected to have been committed and police are called to the health care facility
- if permitted or required by law (consult Privacy Officer/Legal)
- no disclosure to student's parents without express written consent from student
  - example: parent asks for PHI of son (student) regarding son's recent counselling sessions received at the College and relating to his unusual behavior, unless there is a risk of serious bodily harm to the student or others (first bullet, above), encourage parents to speak to their son or meet with counsellor and son together, if son permits

PHIPA Access/Correction Request Procedure

- Request to be made to Department Head of College Health Services
- Privacy Officer will direct requests to Department Heads
- Co-ordinate response between Department Heads when necessary
- If request made by Substitute Decision-Maker (hierarchy)

- No right to access
  - Quality of care data
  - PHI needed for Quality Assurance programs
  - Raw data from psychological tests or assessments
  - PHI used solely for research

Requests for Correction (applies to PHIPA and FIPPA)

- Requester has right to request correction if believe it to be inaccurate or incomplete and reason for belief is given in written request
- College has obligation to correct if inaccurate or incomplete for the identified purposes
- Department Head responsible for processing the correction request but may consult with the Privacy Officer
- Request must be written and state it is under PHIPA/FIPPA; fees must be paid
- Respect 30 day time limit for response
- If inaccurate or incomplete, Requester can give College the necessary additional information
- Procedure for making the correction is very specific – follow College policy
- Notify Requester in writing if denying the request to correct; requester may append statement of disagreement to his or her College record

PHIPA - Access/Correction Procedure

Step 1: can request be granted informally? Routine disclosure? If yes, record date of disclosure and information disclosed in the patient record. Disclose the information not the record; the record is College property.

Step 2: verbal request – encourage written request, under PHIPA, best to use PHIPA request form unless can fill request informally

Step 3: written request - 30 day time limit unless expedited request is made with evidence of need for fast-tracking

- assist requester to narrow scope and permit identification of records
- communicate with requester on ongoing basis
- ensure reasonable search is conducted; record details of search
- identify reasons for withholding records
- consult with Privacy Officer if necessary; verify identify of requester
- provide access to requester upon payment of fee for copies (may be waived)

Denying Access to Requester's own PHI

- Usually discretionary

Some reasons:

- information is subject to legal privilege
- law or court order prohibits disclosure
- PHI was created or collected for legal proceeding
- granting access to PHI could reasonably be expected to result in risk of serious harm to treatment or recovery of the individual
- risk of serious bodily harm to requester or someone else
- frivolous or vexatious request, or made in bad faith
- only limit that part of record that qualifies for the denial – disclose that part of the record that is disclosable

If Denying Access to Requester

- Give written notice to requester within time frame with statement of denial and reason for same and notify requester of his or her right to contact the Information and Privacy Commissioner of Ontario and provide the contact information

Thank you.