College of Occupational Therapists of Ontario

PRESCRIBED REGULATORY EDUCATION PROGRAM: PRIVACY & CONFIDENTIALITY

PREP 2014 – PRIVACY AND CONFIDENTIALITY

This module is organized around the following core statement of privacy principles:

YOU CAN ONLY COLLECT, USE OR DISCLOSE PERSONAL HEALTH INFORMATION WITH THE INFORMED CONSENT OF THE CLIENT OR IF ONE OF THE EXCEPTIONS APPLY

PREP MODULE: PRIVACY AND CONFIDENTIALITY

Complete the Reflective Practice Exercise 2 online in the Practice Development Portal.

YOU CAN ONLY COLLECT, USE OR DISCLOSE PERSONAL HEALTH INFORMATION WITH THE INFORMED CONSENT OF THE CLIENT OR IF ONE OF THE EXCEPTIONS APPLY

1. INTRODUCTION

Privacy encompasses much more than confidentiality.

Confidentiality of client information has been a core value of health care providers for centuries. Recently, the broader concept of privacy has replaced strict confidentiality constructs. Protecting client privacy entails comprehensively safeguarding personal health information on behalf of the client. With confidence that the practitioner will keep their information private, clients may be more willing to share needed information. It is both professional misconduct[1] and a breach of contract for an OT to inappropriately disclose confidential client information.

The privacy duty requires OTs to appreciate that client information belongs to the client, that it may only be collected, used and disclosed in the client's best interests and that the OT only holds the information on behalf of the client.

In Ontario, the duty of maintaining the privacy of personal health information is established and enforced through the *Personal Health Information Protection Act* (PHIPA). Under PHIPA, the Ontario Information and Privacy Commissioner (IPC) monitors compliance with the Act and receives complaints from members of the public.

---

[1] The following definitions of professional misconduct may apply:

Acts of professional misconduct

1. The following are acts of professional misconduct for the purposes of clause 51 (1) (c) of the Health Professions Procedural Code:
   1. Contravening, by act or omission, a standard of practice of the profession or failing to maintain the standard of practice of the profession....
   5. Giving information about a client to a person other than the client or the client's authorized representative except with the consent of the client or the authorized representative or as required or authorized by law....
   35. Contravening, by act or omission, a federal, provincial or territorial law, a municipal by-law or a by-law or rule of a hospital within the meaning of the Public Hospitals Act in which the member provides services if,
      i. the purpose of the law, by-law or rule is to protect public health, or
      ii. the contravention is relevant to the member's suitability to practise....
   48. Engaging in conduct or performing an act relevant to the practice of the profession that, having regard to all the circumstances, would reasonably be regarded by members as disgraceful, dishonourable or unprofessional.
   49. Engaging in conduct that would reasonably be regarded by members as conduct unbecoming an occupational therapist.

© 2014, College of Occupational Therapists of Ontario

In addition to regulatory liability and to protect against intrusion upon an individual's seclusion, (new privacy tort[2]), OTs that cause damage by disclosing private personal information to others[3] could face financial liability.

The importance of protecting privacy is articulated within the very first competency of the *Essential Competencies of Practice for Occupational Therapists in Canada* and, along with confidentiality, is repeated frequently as a key competency throughout the document. The concept is also a significant component of the College's *Standards for Record Keeping* (three of the twelve standards statements pertain directly to OTs' privacy duties).

This PREP module is intended to assist OTs in recognizing their confidentiality and privacy obligations and ethically applying privacy principles in their individual practice settings.

a. Learning Objectives

When an OT has completed this Module, he or she will be able to:

1. Understand that maintaining confidentiality and ensuring privacy are legal, ethical and professional obligations;
2. Demonstrate an understanding of the relevant aspects of the legislation, *Personal Health Information Protection Act* (PHIPA), *Personal Information Protection and Electronic Documents Act* (PIPEDA), and *Freedom of Information and Protection of Privacy Act* (FIPPA), and be able to apply the concepts and definitions to his or her own practice;
3. Understand the principles of confidentiality, privacy, and transparency and how the relevant legislation can and does impact occupational therapy practice;
4. Identify some of the ethical challenges that OTs might face in practice in the course of their efforts to comply with both the standards and the legislation of confidentiality and privacy;
5. Demonstrate sound knowledge, understanding and applications of the standards and legislation relevant to confidentiality and privacy through a series of practice scenarios.

b. Reflection Practice Exercise 1 (optional)

Assess your understanding of confidentiality and privacy issues by independently answering the following questions. Base your responses on your current beliefs, values and practice experiences. While this reflection can occur in a group setting, it is intended for your personal learning. After completing the module, evaluate your learning by reflecting on these responses. The College does not require you to submit these answers, but recommends that you retain the answers for future reference.

Answer **Yes, No** or **Sometimes** to the following questions or statements:

1. Confidentiality and privacy issues arise in my practice.

   YES NO SOMETIMES

2. If the police contact you about a crime they think your client committed, can you tell them anything?

   YES NO SOMETIMES

---

[2] A "tort" is a civil wrong (as opposed to a criminal wrong) for which a court will award a monetary judgment against the wrongdoer. For example, negligence causing bodily harm and libel and slander are examples of torts.

[3] Jones v. Tsige, 2012 ONCA 32

© 2014, College of Occupational Therapists of Ontario

3. Can you explain your responsibility for your client records when you stop practising?

   YES NO SOMETIMES

4. Can you identify the three most likely, realistic threats to the safeguarding of the personal health information entrusted to you, and the most effective measures to address those risks?

   YES NO SOMETIMES

5. If you misplaced a record containing personal health information while outside of your work setting, would you know what to do?

   YES NO SOMETIMES

6. It is all right to collect personal health information about a client without their prior consent.

   YES NO SOMETIMES

7. Do you know when PHIPA applies to you, when PIPEDA applies to you, and whether it matters which statute applies?

   YES NO SOMETIMES

8. Does the "lock box" apply to your clients' "circle of care"?

   YES NO SOMETIMES

9. Can a client require you to correct an entry in a report written by another practitioner that you happen to have in your files?

   YES NO SOMETIMES

10. Do you know who can give consent for the release of an incapable client's personal health information?

    YES NO SOMETIMES

c. Overview of Privacy and Confidentiality

Consider the following scenario:

Introductory Scenario

A home care client tells you that she would like help in developing strategies to remember to turn off the stove. She has left a pot of food burning more than once in the past month. However, the client does not want her daughter to know because her daughter thinks she is not coping well at home and needs to move into a nursing home. The client also does not want you to tell her physician, as the physician is on the verge of telling the daughter that the mother cannot cope at home. What are your obligations?

This scenario raises the issue of the extent of the client's control over her personal health information.

© 2014, College of Occupational Therapists of Ontario

Clearly, the disclosure by the client is critical to the OT's ability to assist the client. Without this information, the OT cannot provide the assistance the client needs. Family members are not usually entitled to information about the client without the client's consent. The client's physician (but not the client's daughter) is part of the client's circle of care. While there may be circumstances in which disclosure to others within the circle of care can be made without explicit client consent, the client has invoked the "lock box" preventing the OT from sharing that information with the physician.

One issue is whether the client is capable of giving consent on the appropriate use and disclosure of that information. One cannot assume that she is not capable simply because she is elderly, or even because she is having difficulty coping at home by herself. However, the OT may be concerned that the client may not understand and appreciate the reasonably foreseeable consequences of the client's decision to keep this information from her family and physician. The OT should consider further assessment of the client's capacity to make decisions about this information.

Even if the client is capable, the information reveals potential safety concerns about the client's choice to remain at home. In some circumstances, safety concerns can permit disclosure of personal health information without client consent.

The balancing of these competing interests can be summarized in one sentence describing an OT's duty of privacy and confidentiality:

> **You can only collect, use or disclose personal health information with the informed consent of the client or if one of the exceptions apply.**

This sentence captures the essence of privacy and confidentiality. As such, it is reproduced in the header of this module. Every portion of this sentence is laden with meaning and the rest of this module will explore the layers of these meanings.

2. YOU (WHO IS RESPONSIBLE)

While everyone who has access to information in the health context is responsible for ensuring privacy, a fundamental issue is identifying the specific duties of each professional who holds responsibility for the privacy of personal health information.

Health Information Custodians

Under PHIPA, the primary responsibility rests with the Health Information Custodian ("the custodian") providing health care. The custodian is the person or organization responsible for maintaining all health records. An OT is the custodian if he or she is providing OT services to an OT client, unless the OT is acting on behalf of another custodian (e.g., a hospital, another facility or a group practice). The custodian must create, implement and oversee a privacy policy that meets the requirements of PHIPA.

A sole-practice OT is the custodian of any health information that the OT collects. If an OT works for a health organization such as a hospital or long-term care home, the organization is usually the custodian of health information. However, there may be some exceptions. For example, the operator of a multi-

© 2014, College of Occupational Therapists of Ontario

disciplinary clinic or a home care service might choose to act only as the agent of the practitioners, and may require each of them to operate as separate custodians. This is rare, however, as the operator usually wants to maintain control over the physical records and will therefore assume the role as custodian.

For the purposes of complying with PHIPA, two or more OTs working together may decide to act as a single organization such that this organization becomes the custodian of health information. This may allow the OTs to create a single privacy policy governing consistent health record-keeping practices and to share responsibility for complying with PHIPA.

An OT who works for an organization that does not provide health care services (e.g., a school board), will usually have to assume the role of custodian with respect to his or her own health care services.

Usually, the issue of who is the custodian is negotiated by the relevant parties. There are some situations where PHIPA designates the custodian (e.g., a public hospital). In cases where there are more than two OTs working as an organization, it is best to have clear agreement as to who is the custodian and who has responsibility for the records when the relationship ends.

Information Officers

PHIPA requires every OT or other custodian to appoint a contact person (often called an Information Officer or a Privacy Officer) to ensure compliance with the privacy policy and requirements of PHIPA. The Information Officer's duties include reviewing the organization's privacy practices, providing training, and monitoring compliance. The Information Officer is also the contact person for requests for information from clients or the public.

A sole OT usually acts as the Information Officer. A health organization may appoint a person within the organization, or may hire a person outside of the organization to be its Information Officer.

Professional Accountability

The fact that an OT works for an organization that has chosen to be the custodian does not absolve the OT from professional accountability. As an agent (i.e., representative) of the custodian, the OT has a responsibility to be familiar with the custodian's privacy policies and to comply with them. This includes advising clients of the custodian's privacy policies. If the privacy policies are not fully compliant with PHIPA, the OT has a responsibility to advocate for a review and change of the policy. In addition, as an accountable professional, the OT has a duty to intervene if a client's privacy rights are jeopardized. For example, if personal health information is not being kept secure (e.g., closed files are left in boxes in a hallway with public access), the OT is responsible for advocating compliance with privacy obligations. The OT's own personal privacy practices must be above reproach.

Retirement, Sale of a Practice, and Estate Planning

If the OT is the custodian, he or she must make reasonable plans for the security and management of the personal health information when he or she ceases practice. Records must be maintained securely for the suitable retention period (discussed below) and clients must be offered an opportunity to access their records or to have them transferred to another custodian. The easiest solution is when another custodian takes over the practice at the same location. However, even then, clients must be told of the change of

© 2014, College of Occupational Therapists of Ontario

custody. When the practice closes, the OT must either store the records securely or transfer them to another custodian at another location. In either case, the clients need to be informed of the change of location and of how they can access their records easily. If such action is not taken and the OT dies, the estate of the OT carries this ongoing responsibility.

This obligation may be more difficult in alternative practices (e.g., when OTs are conducting third-party assessments or working for school boards). OTs must determine a reasonable means of ensuring secure retention and access. Some options might include transferring the files to one's successor, ensuring secure retention and client access through the third party that the OT is working for (if it is a custodian), or even retaining the files personally and ensuring client access.

The Information and Privacy Commissioner (IPC) has a useful checklist for closing a practice. For example, on the issue of notifying clients, it says, "Where it is not possible to reach every affected individual by direct notification, notify them indirectly by using multiple forms of notification such as posting a notice in the custodian's office, posting a notice on the custodian's website, recording a message on the custodian's telephone answering machine, and advertising in newspapers."[4]

Disregarding this ongoing obligation is not an option. While it may be that the College has limited reach over former members, the College retains jurisdiction to take action for an omission that occurred while registered. That is, the IPC maintains jurisdiction over any custodians, whether retired or not.

3. CAN ONLY (SAFEGUARDING INFORMATION)

OTs need to ensure that inadvertent or even malicious privacy breaches do not occur. A privacy breach has the potential to cause significant harm (real, potential or perceived) to the client and is a fundamental failure of the OT's duties.

Protecting Personal Health Information

Custodians must have protocols for protecting personal health information in their custody or control. Custodians and OTs must take appropriate measures to protect personal health information from unauthorized access, disclosure, use or tampering. These safeguards must include the following components:

- physical measures (e.g., restricted access areas, locked filing cabinets),
- organizational measures (e.g., need-to-know and other staff policies, security clearances), and
- technological measures (e.g., passwords, encryption, virus protection, firewalls).

Custodians and OTs need to review systematically all of the places where they may temporarily or permanently hold personal health information and assess the adequacy of the safeguards for those locations. Consideration should also be given to any discussion of clients where conversations might be overheard. The College's *Standards for Record Keeping* offers specific guidance on the types of safeguards expected of OTs, including for sensitive areas such as travelling with client information and using email.

A custodian's or OT's privacy policy should state how health information will be protected.

---

[4] Checklist for Health Information Custodians in the Event of a Planned or Unforeseen Change in Practice (Information and Privacy Commissioner, May 29, 2007).

© 2014, College of Occupational Therapists of Ontario

Retention and Destruction

Custodians and OTs also need to retain, transfer and dispose of records securely, in accordance with College standards. For example, the College's *Standards for Record Keeping* requires that client records be kept for ten years from the last contact with the client (or, if the client was not an adult at last contact, ten years from when the client turned 18). Performance indicator 7.3 of that Standard reads as follows: "That destruction of a record, both in electronic form and paper, is done in a secure manner that prevents anyone from accessing, discovering or otherwise obtaining the information (e.g., cross-shredding, incineration, etc.)".

Examples of Privacy Breaches

It is instructive to review the Information and Privacy Commissioner's (IPC) website to find illustrations of actual privacy breaches that have resulted in IPC investigations and directives. The sheer volume and variety of real privacy breaches that have come to the attention of the IPC is stunning. They include the following:

- **Numerous examples of personal health information in records put out in the garbage.**
  - One included carbon papers for requisitions.
  - In another, laboratory records containing sensitive personal health information fell off a recycling truck and were found blowing around on the street. The IPC directed that the laboratory set up cross-cut shredding equipment at every location and that use of shredding companies requires a written contract with strict terms including requiring a certificate of destruction for every assignment.
  - One rehabilitation clinic closed, with abandoned files left in the empty premises.
  - A client at a mental health facility asked for scrap paper. On the back of the paper were the names and diagnoses of seven other clients.

- **Many cases of misfiling.**
  - In one, a client was issued a receipt for another client.
  - In a number of cases, clients were provided with a copy of their file which accidentally included pages from other clients.
  - In other cases, files were completely lost in a move.
  - There were a number of cases in which memory sticks were lost.
  - In one case, a practitioner lost her appointment book for home visits. The IPC suggested that minimal personal information should be recorded in appointment books and code should be used where possible.
  - Another practitioner left home visit documents on public transit after searching through her bag for something else, then rushing off the transit vehicle.

- **Misdirected letters, faxes and other electronic transmission of information have also been a frequent issue.**
  - One significant example included mass mailing of cancer screening reports by Cancer Care Ontario by Canada Post where a number of the packages (containing significant personal health information on numerous clients) did not arrive. The IPC recommended that secure electronic means be used in future for this sort of information.

© 2014, College of Occupational Therapists of Ontario

  - Staff at another facility made an error inputting data onto a provincial health data base. The staff inserted the wrong facility number permitting staff at another facility (i.e., the one with the inputted facility number) to view the data.

- **Cases of stolen laptops and other portable electronic devices have been numerous.**
  - The IPC has been particularly concerned about this development, and in 2007, published a Fact Sheet requiring that all portable electronic devices be protected by strong encryption.[5] The Fact Sheet was published after an infamous incident where the laptop of a researcher for the Toronto Hospital for Sick Children was stolen from his vehicle.
  - In one recent case a public health nurse lost a memory stick with information (including name, home address and health number) of over 83,000 people who received immunization injections. The IPC directed that significant measures be taken to prevent a recurrence of such an incident. The IPC also found that the regional health department collected unnecessary information, including health numbers, and directed that such information be securely destroyed.
  - Repeated examples of stolen laptops with information on thousands of clients receive high priority from the IPC resulting in the imposition of stringent directions to the custodian.
  - Custodians are responsible to take appropriate measures to prevent theft of personal health information.
  - The following events have been reported to the IPC:
    - Theft of a package from a courier van when the driver left the door open while making deliveries and pickups.
    - Break-ins into the offices of practitioners.
      Break-ins into the homes of practitioners, resulting in theft of laptops and briefcases.

- **There were numerous cases of staff checking the personal health records of friends and relatives who had been treated at the office or facility. Whether malicious or purportedly "well-intentioned", this is never permissible.**
  - Some of these unauthorized cases have been malicious. In one case involving a domestic dispute, one spouse was admitted to hospital. The other spouse and his new girlfriend work at the hospital. The client alerted the hospital of her concern that there might be unauthorized access attempts. As a result a "VIP" note was put on file alerting all persons attempting to access the file that access was being monitored. The new girlfriend accessed the chart regardless on more than one occasion. The IPC found that the hospital failed to take sufficient efforts to prevent this unauthorized access.
  - Four years later a similar incident occurred again at the same hospital where a technologist reviewed the health records of his ex-spouse's new spouse six times over nine months for no health-related purpose.
  - Some of the unauthorized access breaches were more innocent. In one case, an EEG technician reviewed the client's father's computer chart with the client to ascertain the client's family history. However, the son then saw another, unknown diagnosis of the father which was upsetting to the son.

- **Technology can create unique privacy breach issues.**
  - In one case, a methadone clinic monitored clients giving urine samples by video camera. Clients consented to this monitoring. The camera images from the clinic were picked up by

[5] Fact Sheet #12 - Encrypting Personal Health Information on Mobile Devices, (Information and Privacy Commissioner of Ontario, May 1, 2007).

© 2014, College of Occupational Therapists of Ontario

a back-up camera in a car parking outside the clinic. The images were sufficiently clear to permit a reporter to identify a client's face for an interview when the client left the clinic. The wireless monitoring system was replaced by a wired one.

- In another case, due to a technical glitch, participants in two discrete video conferences were linked inadvertently into one teleconference. As a result, the clients of each teleconference could see one another. The video conferences were terminated immediately and changes were made to ensure that in future, prior teleconferences would end before the next could begin. [6]

- **There have been only a few media and social media complaints to date. In one, an ER physician allowed a reporter to "shadow" him for a day and take photographs for an article about hospital overcrowding. Consent was not obtained from the clients observed by the reporter or who were photographed. A complaint was made by a client who read an article in the newspaper disclosing the client's first name and medical condition.**

OTs should be cautious about using WiFi, Skype or other electronic media that are not secure. Entering personal health information on a device in a publicly accessible "hot zone" may compromise the security of the information.

As the summary above indicates, one of the best ways for OTs to educate themselves about safeguarding personal health information is to review the *Decisions and Resolutions* page of the IPC's website, found at **www.ipc.on.ca**.

Social Media

Social Media Scenario

> *An OT tweets the following: "I have had it with those #!@%* government bureaucrats. An 86 year-old decorated war veteran (and former CFL wide receiver) is falling daily. He lives at home alone. But it is taking weeks to get authorization for his walker. Nobody seems to care anymore."*

This posting contains sensitive health information about someone who may be identifiable to many in the community, perhaps even to complete strangers with Internet search skills. The use of social media creates a number of privacy and confidentiality concerns (in addition to concerns about maintaining professional boundaries). Simply removing the name of a client from a social media posting is not sufficient, in most cases, to protect the client's privacy.

The following questions and guidelines are as applicable to OTs as they are to other professional practitioners. Before making posts to social media, OTs should consider the following:

- Could the information the OT is sharing be used to identify a current or former client?
- Was any of the information the OT is sharing collected during the course of a client relationship?
- What could be the repercussions for the client and the OT if personal health information of a client is revealed?
- Who can view the OT's posts?

[6] This case raises the question about what was different here from the common situation of clients meeting other clients in the waiting area of an office or facility. Client names are often called out into the waiting area which provides even more disclosure than occurred in the videoconferencing example.

© 2014, College of Occupational Therapists of Ontario

In all circumstances, OTs should:

- Conduct themselves online as professionals – just as they would in the community;
- Manage the privacy and security settings of the OT's social media accounts. Privacy settings can shift and change without notice. Check the settings frequently;
- Assume that information an OT posts can be accessed or altered by others;
- Ensure that the privacy settings for content and photos are set appropriately and monitor who is able to post to any of an OT's social media locations. Clients should not be among those who are allowed to view or post. Remember, no privacy mechanism is guaranteed;
- Regularly monitor all content an OT or others post to an OT's social media accounts and remove anything that is inappropriate;
- Ask others not to tag an OT on any photographs without the OT's permission;
- Ask others to remove any undesirable content related to the OT.[7]

OTs are not prohibited from using social media. However, the responsible use of social media is essential for privacy purposes. Defining "responsible" is one of the ethical, professional and legal challenges facing OTs. This responsibility is compounded by the fact that the privacy values of fellow users vary widely by age, personal experience and personal beliefs. When it comes to social media, OTs must put the privacy interests of their clients ahead of their own personal interests of self-expression.

Responding to a Privacy Breach

Responding to a Privacy Breach Scenario

> *An OT who works in the motor vehicle accident practice area mails out two of his reports that are long overdue. He is in a bit of a rush and puts the reports in the wrong envelopes. Two days later, he receives a call from one insurer who says that the letter contains the wrong report. The OT calls the other insurer who confirms that it, too, received the wrong report. The reports contain the name, home address and detailed personal health information of each client. What should the OT do?*

There is a three-step response to privacy breaches: contain, disclose, reflect:

Contain: Whenever there is a privacy breach, the first priority is to limit the breach. In this scenario, the OT should ensure that the reports are returned by the insurers in a secure manner, and that they have made no copies or notes on them. Alternatively, if the recipient is responsible, having them securely destroy the reports (e.g., cross-cut shredding) and certifying that they have done so (and made no copies or notes) might also be appropriate.

Disclose: Section 12 of the PHIPA requires that the client be notified at the first reasonable opportunity when information is stolen, lost or accessed by an unauthorized person. The manner of notification needs to be appropriate to the circumstances. In the scenario above, with only two clients involved, telephone notification explaining the privacy breach and its implications for the client and answering any questions might be appropriate. A letter might also be sufficient.

---

[7] See: Nursing 2.0, (Ontario College of Nurses of Ontario, (*The Standard*, Fall 2011, Volume 36, Issue 3)), and *Professional Advisory – Use of Electronic Communication and Social Media*, (Ontario College of Teachers, February 23, 2011).

© 2014, College of Occupational Therapists of Ontario

In some circumstances (e.g., when dealing with vulnerable clients, such as those with serious mental illnesses), personal notification at the next scheduled therapeutic visit might be more appropriate. The notification process can be time-consuming and expensive. In some cases, the custodian must hire professionals to locate clients who are no longer reachable at the contact information on file with the custodian.

Reflect: A third obligation is for the custodian to review its privacy policies and practices to make changes preventing such a privacy breach from happening again. This may be a good opportunity to review the organization's entire approach to privacy to ensure that it is sufficiently comprehensive and robust.

There is no requirement to notify the IPC of a privacy breach, particularly if it is relatively minor, quickly contained and handled responsibly. However, where the privacy breach is significant, or where the IPC is likely learn of it anyway, it may be prudent to involve the IPC early on in the process. The expertise and resources of the IPC can assist in handling each aspect of the response to the privacy breach. The custodian should expect feedback and, in many cases, even direction from the IPC on upgrading privacy policies and practices.

4. COLLECT, USE OR DISCLOSE

A custodian's privacy policy should clearly explain how and when personal health information will be collected, used and disclosed.

a. Collection of Information

Generally, an OT should collect personal health information directly from the client. Indirect collection (e.g., from existing health records, from family members) may reduce the client's ability to control the use of their personal health information. However, in some circumstances (e.g., third-party assessment, in order to enhance the accuracy and completeness of the information available for an OT) indirect collection is indicated. If feasible, indirect collection should be done with the consent of the client, and should be confirmed with the client for accuracy.

OTs should be conscientious when information is routinely collected from third parties before the OT meets the client for a first visit. This scenario often occurs in the context of third-party assessments or services provided in schools. The OT should consider whether it is really necessary to obtain the information indirectly in advance of the first visit. The answer may be "yes", but that is not automatically the correct answer.

There are circumstances in which collecting personal health information from the client directly is not feasible (e.g., in some formal research projects).

Even the informal obtaining of information about a client can amount to "collection". Just because the information is not recorded does not mean that it was not collected. For example, discussing a client's capabilities with a family member while the client is changing in another room constitutes collecting personal health information. This example raises the issue of how to determine when indirect collection of personal health information is appropriate.

© 2014, College of Occupational Therapists of Ontario

b. Use of Information

Use of personal health information occurs internally within the organization (i.e. the custodian). Disclosure refers to circumstances in which the information is shared externally to the organization. Even within the organization, the client's personal health information should be used only for the purposes for which it was collected (e.g., treatment) and for functions deemed reasonably necessary to carry out that purpose (e.g., a clerk entering clients' personal health information into the record-keeping system).

Otherwise, the client must consent to the use of the information unless one of the exceptions, discussed below in section 7, applies. An example of when consent would be required is including a picture of the treatment of the client in an internal email or newsletter intended only for staff.

Use of Information Scenario

An OT is asked to assess a client's work capabilities in a Workplace Safety and Insurance Board (WSIB) matter. The OT is sent a package that includes a surveillance video of the client and is asked to keep the video confidential.

This scenario raises complex privacy and ethical issues. Since the OT is assessing the client, he or she has professional obligations to the client. Privacy principles apply. The OT should not agree to withhold personal health information from the client and, if the OT elects to proceed with the assessment, the OT probably should view the video in the presence of the client. For further information, see the College's *Guideline: Use of Surveillance Material in Assessment*.

c. Disclosure of Information

Again, the general rule is that an OT can only disclose personal health information to a third party with the client's consent. Here, disclosure means intentional disclosure. Inadvertent disclosure is a privacy breach resulting from inadequate safeguards. There are some exceptions permitting disclosure without the client's consent. These are discussed in section 7. Disclosure of aggregate information that does not identify the individual is acceptable because it is not personal health information.

5. PERSONAL HEALTH INFORMATION

PHIPA generally applies only to personal health information[8]. Thus, it is important to understand what is captured by the term.

Personal Health Information Scenario

An OT has a side business presenting "LiveWell" seminars for retired members of the community. The seminars involve education in keeping active, being social and getting proper nutrition. The seminar is offered to members of the community, the vast majority of which have never been clients of the OT in the past. Attendees are not individually assessed and the information provided is generic. Are the registration, attendance and billing records for these seminars considered personal health information?

[8] PHIPA also applies to other information that is mixed in with personal health information. For example, if the OT organizes adventure tours and, contrary to recommended practice, happens to keep that information mixed in with clients' clinical files, this also becomes personal health information.

© 2014, College of Occupational Therapists of Ontario

In all likelihood, these seminars would not be considered "health care". While there is a fine line between health prevention and promotion services on the one hand, and lifestyle education on the other, this scenario appears to fall into the latter category. However, while PHIPA may not apply to the OT, in all likelihood, the federal privacy statute, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to these activities. So, privacy of personal information must still be protected.

a. What is Personal Health Information?

OTs have a legal and professional duty to protect the privacy of clients' personal health information. Personal health information refers to almost anything that would be in an OT's files on a client related to health care. Personal health information is defined in PHIPA as written or oral identifying information about a person, if the information:

(a) Relates to the person's physical or mental health, including the person's family health history;
(b) Relates to the providing of health care to the person, including the identification of a person as someone who provided health care to the person;
(c) Is a plan of service within the meaning of the *Home Care and Community Services Act* (1994) for the person;
(d) Relates to the person's payments or eligibility for health care, or eligibility for coverage for health care;
(e) Relates to the donation by the individual of any body part or bodily substance of the person, or is derived from the testing or examination of any such body part or bodily substance;
(f) Relates to the person's health number; or
(g) Identifies a person's substitute decision-maker.

Where the information does not identify the client, it is not personal health information. However, identifying information is not limited to the client's name. OTs must be sensitive to the fact that clients can be identified by descriptive details, not just by name. If the information can be combined with other data to identify the client, it is personal health information. For example, using a client number on a file that can be combined with the facility's master list to identify the client makes the data personal health information to anyone with access to the master client list.

b. Non Health-Related Personal Information

When the information is not personal health information, OTs need to ask if it is still personal information to which PIPEDA applies. PIPEDA is a federal law that governs the collection, use, and disclosure of personal information in relation to commercial activity outside of the health care community.

PIPEDA applies only to commercial activities of OTs, such as the sale of products and the offering of educational sessions. Unlike PHIPA, which governs personal health information, PIPEDA governs all types of non-health personal information. Examples of personal information include the person's name, date of birth, and home address.

© 2014, College of Occupational Therapists of Ontario

The following ten privacy principles apply to OTs' commercial activities:

1. **Accountability:** Someone in an organization (the "privacy officer", sometimes called an "information officer") must be accountable for the collection, use, and disclosure of personal information. The privacy officer must develop privacy policies and procedures, and ensure that staff receives privacy training.
2. **Identifying Purposes:** An organization must identify the purposes for which personal information will be used at the time that the information is collected.
3. **Consent:** Informed consent is required to collect, use, and disclose personal information except in limited circumstances (e.g., in emergencies, or where the law otherwise permits this).
4. **Limiting Collection:** An organization must only collect the information that is necessary to collect for the identified purposes.
5. **Limiting Use, Disclosure, and Retention:** An organization must only use, disclose and retain personal information that is necessary for the identified purposes and that is obtained with consent. It should be retained no longer than necessary.
6. **Accuracy:** An organization must make reasonable efforts to ensure that any personal information collected is accurate, complete, and up-to-date.
7. **Safeguards:** An organization must protect personal information with appropriate safeguards in order to protect against loss, theft, unauthorized access, disclosure, copying, use, or modification.
8. **Openness:** An organization must make its privacy policies readily available.
9. **Individual Access:** Upon request, an individual must be informed of the existence, use, and disclosure of his or her personal information, and be given access to it. An individual can request corrections to the information. Access may be prohibited in limited circumstances such as protecting the privacy of other persons, in the event of a prohibitive cost to provide it, or other legal reasons.
10. **Challenging Compliance:** An organization must have a complaints procedure relating to personal information and must investigate all complaints.

As one can see, PHIPA and PIPEDA are based on the same principles. PHIPA simply provides more details about how to achieve these principles in the health care context.

6. WITH THE INFORMED CONSENT OF THE CLIENT

Unless an exception applies, an OT can only collect, use and disclose personal health information with the consent of the client. To be valid, the consent must be informed. Consent can be implied or expressed (i.e., verbal or written). In some circumstances, implied consent is not sufficient.

a. Informed Consent

The requirement of consent by the client is the cornerstone of the privacy principle that a client controls his or her personal health information. That control extends throughout the therapeutic process from initial collection of the information, to its use, and extending to any subsequent disclosure. Client control of their personal health information also means that clients can request access to it and correct errors in the information.

© 2014, College of Occupational Therapists of Ontario

COMPONENTS OF INFORMED CONSENT

Many of the principles of informed consent for treatment apply to consent relating to personal health information. The client must understand the purpose of the collection, use and disclosure, and must appreciate that they have a choice about whether to give consent and that they can withdraw consent later on. The consent must relate to the information under discussion and must not be obtained by deception or coercion.

Thus, consent given for one purpose (e.g., to assess and treat the client) cannot be used for another purpose (e.g., the marketing of one's other activities, like the "LiveWell" scenario described above).

Client consent can be implied for the collection and use of information, so long as the above requirements are met (typically, where the information is used only for the purpose of assessment and treatment). The ability to rely on implied consent is enhanced when the custodian makes its privacy policies readily available to clients, describing how such information is generally handled. Disclosure of personal health information, however, must be expressed (i.e., verbally or in written form) unless the disclosure is only to another custodian for the purpose of treatment. For example, disclosure to an insurer requires expressed consent.

These principles mean that the informed consent process has to be more extensive for some practice models. For example, third-party assessments require a detailed explanation of the purposes of collecting the information and of how it will be used and disclosed. The principle of a client being able to withdraw consent also becomes more significant in that context. An OT working for a government funding agency, an employer or a medical device supplier would need to carefully explain his or her role and the purposes for which personal health information will be used if the OT enters into any sort of OT-client relationship.

A client cannot, however, impose conditions on their informed consent that require an OT to compromise his or her professional standards. For example, an OT must refuse a client's request that the OT not record any information about the client in the OT's notes. In that circumstance, the client has to decide whether to give consent to record unconditionally or to withhold consent for treatment entirely.

CIRCLE OF CARE

The "circle of care" concept is a prime illustration of implied consent for disclosing personal health information. An OT can share personal health information obtained from the client for health care purposes with other custodians within a client's circle of care without the client's expressed consent.

For example, an OT who is working in a multidisciplinary setting may share personal health information with other health care professionals who are providing care to the same client because these other health care professionals are within the client's circle of care. Similarly, an OT who refers a client to another health professional may consider that health professional to be within the client's circle of care.

The circle of care of a sole OT's client may also include other health care providers in other institutions if a) it is necessary for providing health care to the client, and if b) it is not reasonably possible for consent to be obtained in a timely manner. However, many OTs do not share information with others on the health care team without the client's explicit consent unless there is some urgency or other good reason so as to avoid misunderstandings. This caution is particularly important when the information is sensitive.

© 2014, College of Occupational Therapists of Ontario

The circle of care does not require OTs to disclose information, but simply allows OTs to do so when it is in the best interests of the client.

Circle of Care Scenario

> *An OT receives a telephone call from a registered nurse at a local hospital. The nurse advises the OT that the OT's client, who has dementia and is incapable, has just been admitted to the hospital. The nurse reports that he has been unable to contact the client's substitute decision-maker (SDM). The nurse wants to know about what treatment the OT has been providing to the client. The OT tells the nurse about the treatment and discloses the contact information the OT has for the SDM.*

In this case, the circle of care principle allows the OT to disclose the client's personal health information without expressed consent, and it would be inappropriate to insist that a consent form be signed before making any disclosure.

The exception to this principle occurs if a client says that he or she does not want the information to be shared. In this case, implied consent no longer exists (see discussion below).

For further information on the topic, see the best practices and professional guidelines document published by the Information and Privacy Commissioner of Ontario entitled *Circle of Care: Sharing Personal Health Information for Health-Care Purposes*.

THE LOCK BOX

When a client asks an OT not to disclose certain information about the client to others, the OT must respect that request. This includes requests not to disclose the information to others in the client's circle of care. However, when the OT believes that a person providing treatment needs to know the information that has been omitted from the record in order to provide appropriate care, the OT can inform that practitioner that relevant information is missing from the file. The OT cannot disclose the content of that missing information. However, the treating practitioner is then alerted to the concern.

The lock box can be used to limit access to either 1) all of the client's personal health information or 2) only certain practitioners, (e.g., "don't tell my medical doctor this"). The client can also change his or her mind about opening or closing the lock box, but any disclosure that has already been made cannot be reversed.

The lock box requirement creates challenges for maintaining records. The custodian needs a system for maintaining such records while preventing access to that information by those excluded from accessing it.

ACCESS BY CLIENT

Every client has a right to access his or her own personal health information. This principle was established by the Supreme Court of Canada in 1992.[9] This means that the client has a right to access the entire file, including information provided by third parties (e.g., other practitioners).

There are only a few exceptions to this general principle, including the following:

[9] McInerney v. MacDonald, [1992] 2 S.C.R. 138.

© 2014, College of Occupational Therapists of Ontario

- Instances in which granting access would likely result in a risk of serious harm to the client's treatment or recovery, or a risk of serious bodily harm to the client or another person. The phrase "bodily harm" may include mental or emotional harm.
- Instances in which the information constitutes quality of care or quality assurance information. This is a narrow exception that applies to formal programs established for the general enhancement of health care services under either the *Quality of Care Information Protection Act* or the RHPA.
- Instances in which the information consists of raw data from standardized psychological tests or assessment.

If disclosure of certain information can be withheld from the client, the OT should black out (on a copy, not the original) those parts that should not be disclosed to the client, if it is reasonable to do so, so that the client may access the rest of the record.

The IPC may be asked to review the custodian's refusal to provide a client access to parts of his or her record.

The custodian can charge a reasonable fee for providing a client with access to the parts of his or her medical record she/he is entitled to view. However, in one case the IPC dealt with the issue of charging a reasonable fee for a client's request for a copy to her chart. The chart consisted of 34 pages of psychological documents and the practitioner charged $125. The IPC concluded that this charge was unreasonable. She found that it should take no more than fifteen minutes to review the records to ensure that no information should be severed. Her guideline was that a fee of $30 was reasonable for a chart that was twenty pages or less and that a photocopy charge of 25 cents for every page beyond 20 was reasonable.

Correction Requests

Correction Request Scenario

> *At the end of a home care assessment, a client asks to look at the OT's notes. The OT complies and assists the client in reading her handwriting and understanding the abbreviations used. The client asks the OT to make two corrections. The first is to clarify that the client walks to the corner store and only uses the taxi for grocery shopping at the local superstore. The second is to alter the OT's recommendation from a walker to a power chair.*

This scenario highlights the access rights of the client and raises the issue of what types of corrections an OT must make to his or her records.

Generally, clients have a right to request corrections to errors in their information. An OT that receives a written request to correct an error must respond to it by either granting or refusing the request within 30 days. It is wise for OTs to respond to verbal requests as soon as possible.

Corrections to records must always be made in a way that allows the information in the original record to continue to be legible. The original record should never be destroyed, deleted, or blacked out.

At the client's request, the OT (or custodian) should advise anyone to whom the OT has disclosed the information of the correction. The exception to this is if the correction will not impact the client's health care or otherwise benefit the client.

© 2014, College of Occupational Therapists of Ontario

The OT (or custodian) may refuse the request if the OT believes the request is frivolous or vexatious, if the OT did not create the record and does not have the knowledge, expertise and authority to correct it, or if the information consists of a professional opinion made in good faith. In the example above, corrections are limited to factual information, not professional opinions.

An OT who refuses to make a correction must notify the client in writing, with reasons, and advise the client that he or she may:

- prepare a concise statement of disagreement that sets out the correction that the OT refused to make;
- require the OT to attach the statement of disagreement to his or her clinical records, and disclose the statement of disagreement whenever the OT discloses related information; and
- require the OT to make all reasonable efforts to disclose the statement of disagreement to anyone to whom the OT has previously disclosed the record.

b. Who is the Client? (Substitute Decision-Makers)

Who is the Client Scenario

> *An OT working in a long-term care setting has a client with severe dementia. The OT is able, with minimal assessment, to determine that the client cannot give the OT any meaningful instructions. The client has two children, a son and a daughter, who both want to make decisions for their father. They both call the OT, separately, before the OT's first visit with the client, insisting that only they, and not their sibling, be given the OT's report. The client's daughter has the client's power of attorney for care and the son has the client's power of attorney over the client's property.*

The answer to this scenario may surprise some OTs. As will be seen below, the two types of power of attorney have equal status when it comes to decisions about the collection, use and disclosure of person health information (i.e., privacy decisions). The OT would probably advise the siblings to work out their differences. Otherwise the Public Guardian and Trustee would have to make the privacy decision.

Usually, it is obvious who the client is. In the privacy context, it is the individual about whose health the information has been collected. However, where a client is not capable of making the privacy decision in question, a substitute decision-maker will make the decisions on behalf of the client. The approach to substitute decision-makers for privacy purposes is quite similar to the approach for treatment decisions. The major difference is that personal health information is treated like property. For example, a power of attorney for property, as well as a power of attorney for treatment, can act as a substitute decision-maker.

Another major difference from treatment decisions is that the client can authorize another person to make their privacy decisions even when/if the client is capable.

As with treatment decisions, a client is presumed to be capable unless the OT has reason to doubt the client's capacity. Where there is a doubt, the OT should assess whether the client understands the privacy issue at stake and appreciates the reasonably foreseeable consequences of that decision. If the OT determines that the client is not capable of making the privacy decision, the OT should inform the client when this is feasible. The client has the right to have that determination reviewed by an independent board.

© 2014, College of Occupational Therapists of Ontario

The ranking of substitute decision-makers is as follows:

- Guardian (for either care or property)
- Power of attorney (for either care or property)
- Representative appointed by the Consent and Capacity Board
- Spouse or partner
- Child or custodial parent
- Access parent
- Brother or sister
- Any other relative
- Public Guardian and Trustee

The highest-ranking substitute who is able and willing to make the decision is the substitute decision-maker.

7. OR IF ONE OF THE EXCEPTIONS APPLY

There are a number of exceptions to the above rules. Most of the exceptions are contained in PHIPA itself. Others are created or recognized by other statutes that intersect with PHIPA.

(a) PHIPA Exceptions to the Requirement of Informed Consent

There are a number of circumstances when personal health information can be collected, used or disclosed without the client's consent. In fact, when/if these exceptions apply, the collection, use and disclosure can be made contrary to the explicit instructions of the client. For example, the lock box direction from a client can be disregarded where an exception applies.

EXCEPTIONS TO **COLLECTION** OF PERSONAL HEALTH INFORMATION WITH CONSENT

There are very few exceptions to the requirement to have the client's consent to collect information about the client. As described above, indirect collection of personal health information is permissible if it is necessary for providing health care to the client and when obtaining the information directly from the client is not feasible. Another exception is for formal research projects (i.e., those approved by a Research Ethics Board).

EXCEPTIONS TO **USE** OF PERSONAL HEALTH INFORMATION WITH CONSENT

There are some exceptions when the custodian can use personal health information without the client's consent. For example, the information can be used for program planning purposes (e.g., a review of the practice's operations to see if bidding on a CCAC contract is feasible), quality assurance activities (e.g., a supervisor reviewing a probationary OT's files), training purposes (e.g., an in-service review of best practices), to prepare for legal proceedings (e.g., responding to a complaint by the client) and for billing purposes.

EXCEPTIONS TO **DISCLOSURE** OF PERSONAL HEALTH INFORMATION WITH CONSENT

There are many exceptions permitting disclosure to be made without the client's consent. A significant one is that an OT may disclose a person's personal health information if the OT believes on reasonable grounds that the disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm

© 2014, College of Occupational Therapists of Ontario

to the person or anyone else. For example, if an OT reasonably believes that a client is incapable of driving safely and that the client will likely drive, the OT can inform the proper authorities. This is true even though the OT is not required by the *Highway Traffic Act* to make such a report in the way that physicians and optometrists are. Another significant example is disclosure of a child in need of protection.

A related exception permits an OT to assist investigators and inspectors acting under statutory authorization (e.g., police officers undertaking a criminal investigation; occupational health and safety inspectors) without client consent, even if the client is the subject of the investigation. Disclosure in these circumstances is discretionary (unless the investigator has legal authority to compel cooperation) and the OT needs to balance the benefits of providing assistance against the potential harm to the client by making such disclosure. The OT can assist the investigation even if the OT is not asked for assistance (e.g., if the OT learns in the media about the investigation and realizes that he or she has important information). The legislation is not directive about whether the OT can make disclosure if an investigation has not yet begun (e.g., information about a crime not known to the authorities); however, in those circumstances the OT would not normally consider making disclosure unless the significant risk of serious bodily harm exception, discussed above, already applies.

PHIPA specifically **permits** disclosure of personal health information that is permitted or required by many other acts, including the following:

- Under the *Health Care Consent Act* or *Substitute Decisions Act* for the purposes of determining, assessing or confirming capacity;
- To a college governed by the *Regulated Health Professions Act* (RHPA), either voluntarily or in order to make a mandatory report required under the RHPA;
- To the Ontario College of Social Workers and Social Service Workers (e.g., to report the conduct of a Social Worker, as they do not fall under the RHPA);
- To the head of a psychiatric facility regulated under the *Mental Health Act* for the purpose of assisting in the treatment of a client or to assist in a decision about the custody, detention or release of the client; and
- To make a report under the *Child and Family Services Act* about a child in need of protection.

Personal health information may also be disclosed for the purposes of contacting family members, friends, or other persons who may be potential substitute decision-makers if the individual is injured, incapacitated, or ill, and cannot provide consent. This may be particularly relevant for OTs working in acute care and long-term care settings, although the issue of an incapable client can occur in any setting.

If an OT is selling his or her practice, he or she can provide the prospective purchaser with access to the client files so that the prospective purchaser can perform a due diligence evaluation of the practice. However, in that circumstance, the prospective purchaser must agree to keep the information confidential.

Disclosure Of Information Scenario

The police are investigating a bank robbery. They show an OT a video of the robbery. The robber is wearing a mask. However, he has a pronounced limp. The police ask the OT if this person in the video is one of her clients because a witness has tentatively identified the bank robber and knows that OT has assessed him for assistive devices. The OT is pretty sure the bank robber in the video is her client.

© 2014, College of Occupational Therapists of Ontario

This scenario falls within one of the exceptions for disclosure without client consent (to assist in a criminal investigation). However, under PHIPA, such disclosure is discretionary, not mandatory. Although OTs are not an extension of the police, the OT would balance the competing interests before disclosing personal health information. On the one hand, OTs should assist police in protecting the public from violent criminals. On the other hand, unnecessary disclosure of personal health information will undermine the willingness of clients to approach OTs for services and to be candid with them. The OT needs to use professional judgment to make decisions based on the College's *Code of Ethics*. OTs can request a court order (i.e.: subpoena, search warrant) or the written permission of the client prior to sharing this information.

(b) Exceptions to the Requirement of Informed Consent Related to Other Statutes

There are a number of other statutes that intersect with PHIPA in some way. Some of the more significant ones for OTs are as follows:

Freedom of Information and Protection of Privacy Act (FIPPA)

PHIPA deals with the collection, use and disclosure of personal health information by health **care providers**. FIPPA deals with the collection, use and disclosure of personal information by a government institution. In a public hospital setting, they intersect because the hospital is both a health care provider and, as of 2007, has also been designated as a government institution.

The general approach is that clinical information is generally governed by PHIPA, while non-clinical information is generally covered by FIPPA. PHIPA generally takes priority over FIPPA statutes. Therefore, an OT assessing or treating clients as an employee of a public hospital would follow the PHIPA rules, starting with determining the custodian within the organization.

The main difference between PHIPA and FIPPA is that the latter allows for public access to the institution's information, which is why the priority of PHIPA is important for protecting client information. For hospitals, FIPPA is primarily relevant for non-clinical information, such as use of public funding, the types of services that will be provided and the policies and procedures followed by the hospital. FIPPA may also come into play when an employee is seeking access to his or her human resources file. FIPPA has special provisions that protect against public access to quality assurance information and research processes and the offering of privileges to staff. FIPPA also has provisions permitting the use of personal information for fundraising purposes.

Mental Health Act (MHA)

The relationship between the MHA and PHIPA is complex. While notionally, PHIPA takes priority over the MHA, there are broad provisions within the MHA that exclude the application of PHIPA. For example, s. 34.1 of the MHA provides psychiatric facilities with extensive powers to collect, use and disclose information about clients without the client's consent. In addition, substitute decision-makers appointed under the MHA prior to PHIPA came into force can continue their role. As noted above, OTs can disclose information to the head of a psychiatric facility under the MHA without the consent of the client to facilitate treatment, custody, detention and release decisions by the facility.

Workplace Safety and Insurance Act (WSIA)

WSIA provides for the assessment, treatment and compensation of workers injured during their employment. PHIPA generally takes priority over the *Workplace Safety and Insurance Act*. However, one exception relates to the disclosure of information about worker claims. OTs cannot rely

© 2014, College of Occupational Therapists of Ontario

solely on PHIPA to permit disclosure of information about workers they are assessing or treating for an employer for WSIB purposes. The confidentiality provisions of the *Workplace Safety and Insurance Act* may apply in some circumstances, particularly where the OT is acting as a representative of the employer. [10]

8. ETHICAL CONSIDERATIONS

The core OT value of respect is consistent with the application of privacy principles in an OT's practice. Privacy concepts are embedded in the principles of client-centred practice, respect for autonomy and collaboration and communication.[11]

Client-Centred Practice

Treating a client's personal health information as the property of that individual to be used for the benefit of that person is the beginning of client-centred practice. From this starting point, the welfare of the client becomes the focus of the therapeutic relationship. For example, an OT will not use the client's information to market other products and services to the client without the client's prior permission, even for organizations that the OT believes would serve the client's best interests.

As was discussed in section 7, there are occasions when an OT will have to use or disclose the client's personal health information without the client's consent. Protecting individuals from harm can, depending on the circumstances, override the duty of confidentiality. For example, if an OT becomes aware of a child in need of protection, the child welfare authorities must be notified. However, mandatory reporting situations are relatively rare.

Ethical dilemmas arise when an OT has a discretionary ability to disclose personal health information to third parties without client consent. For example, when a client seen on home visits (in cases where the long-term care mandatory reporting requirements do not apply) discloses that her son is draining her bank account since she gave him signing authority, the OT **may** report the conduct to the police. In this case, the OT needs to balance the benefit of ensuring that the client's financial situation is protected against the potential harm to the client of making the disclosure without the client's consent.

Privacy can also be breached when clients are called out from a waiting area to see an OT. Calling out the client's name often discloses not only their identity but, in many cases, something about their condition. Strategies to respect privacy and dignity are challenging to develop. OTs should consider all available options including developing techniques to identify and approach a client individually, calling out a first name only, or using technology (e.g., a beeper) to address the privacy concerns as effectively as circumstances permit.

Respect for Autonomy

An OT respects autonomy by enabling the client's right to control who has access to their personal health information. In this context, client autonomy refers to the ability of the client to choose who will have information about the client's health. As has been discussed, the client can have some or all of the information put into a "lock box" to ensure that specified others within the client's circle of care do not

---

[10] Subsection 181(3) of the Workplace Safety and Insurance Act reads as follows:
(3) No employer or employer's representative shall disclose health information received from a health care practitioner, hospital, health facility or any other person or organization about a worker who has made a claim for benefits unless specifically permitted by the Act.

[11] See p. 2 of the COTO *Code of Ethics – Commitment to Good Practice* and pp. 8-10 of the COTO *Guide to the Code of Ethics*.

© 2014, College of Occupational Therapists of Ontario

have access to the "locked" information. The OT must do this even if the OT thinks that restricting access to the information will compromise the ability of the rest of the health care team to provide effective care.

Of course, the OT should discuss the implications of invoking the "lock box" with the client. An ethical issue is the nature and extent of this discussion. Should the OT simply point out the likely consequences and be supportive of the client's right to choose? Or should the OT strongly encourage the client to change his or her mind? This decision involves a balancing of many factors, including the vulnerability of the client, the reasons for the client's decision, the degree of risk created to the client's care and the need for maintaining the client's trust for effective OT care.

Indeed, in every area of privacy in which client consent is required, this "respect for autonomy" principle applies.

Collaboration and Communication

Consent for the collection, use and disclosure of personal health information is the foundation of privacy. Informed consent from a client requires significant collaboration and extensive communication with the client to ensure that the client understands the consequences of his or her decision to disclose personal health information and his or her right to withdraw consent at any time.

An ethical issue arises when an OT is able to use or disclose information without consent. The OT is not required to advise the client in advance of the disclosure, and is not even required to inform the client that the disclosure has been made unless the client asks. In deciding whether to tell the client of the disclosure and, if so, to advise the client before or after the disclosure is made requires a balancing of ethical considerations. Principles of transparency and client-centeredness must be balanced against any harm that can result from the disclosure (e.g., jeopardizing the privacy or safety of third parties).

Other ethical issues occur when an OT concludes that a client is not capable of making decisions about the client's personal health information. The OT needs to consider how frank to be in explaining this determination to the client. The OT also needs to consider to what extent the client should be involved in the discussions with the substitute decision-maker about the client's personal health information. The OT will balance the benefit of including the client as much as possible in these discussions against the discomfort it will cause the client. The OT also needs to consider whether the OT's (or substitute decision-maker's) personal comfort level is influencing the OT's decision.

Thus, privacy principles involve significant ongoing ethical considerations.

9. CONCLUSION

OTs should approach situations with the understanding that personal health information belongs to the client. When OTs recognize that they hold the client's personal health information "in trust" for the client, their confidentiality and privacy obligations may seem a lot less complicated. Following the eight-step process[12] in the College's *Conscious Decision-Making in Occupational Therapy* document is particularly important in the confidentiality and privacy context. Privacy is a core professional, ethical, and legal obligation for OTs.

---

12 The eight steps are as follows:
Step One: Describe the situation.
Step Two: Identify the principles related to the situation.
Step Three: Identify the relevant resources to assist with the decision-making.
Step Four: Consider if you need further information or clarification.
Step Five: Identify the options.
Step Six: Choose the best option.
Step Seven: Take action.
Step Eight: Evaluate the decision.

10. REFLECTIVE PRACTICE EXERCISE SCENARIOS AND QUESTIONS

The following scenarios offer an opportunity to apply the concepts in this module to circumstances that simulate clinical situations. They are not intended to test your knowledge; instead, the scenarios allow you to evaluate whether you understand the relevant principles.

As in resolving confidentiality and privacy duties in occupational therapy practice, there may be more than one appropriate resolution or answer. See Appendix B for best responses to the following scenario questions.

SCENARIO 1:

Dero, an OT, operates a private practice. He has two support staff, two OT employees and a psychologist who assists with some cognitive assessments. Dero recognizes that he is the health information custodian at the practice. Which of the following is his responsibility as the custodian under the *Personal Health Information Protection Act* (PHIPA)?

(a) Hiring an outside person as Information or Privacy Officer.
(b) Creating and implementing a privacy policy for an organization.
(c) Reporting to the Information and Privacy Commissioner whenever a new staff person is hired.
(d) Creating and implementing a workplace violence policy for an organization.
(e) Ensuring that the filing cabinets are locked before he goes home.

SCENARIO 2:

Dero (from Scenario 1) goes with his spouse to make a will. Dero's lawyer asks what his instructions are about his practice should he die suddenly. Which of the following options best respects his confidentiality and privacy obligations?

(a) Inserting into his will a clause that the College should be notified of his death and be asked to en sure that his client files are transferred to another OT.
(b) Inserting into his will a clause that the OTs at his practice at the time should divide the client files among themselves.
(c) Inserting into his will a clause that his estate takes custody of his files and makes arrangements to transfer them to another OT willing to take responsibility for his practice.
(d) Inserting a clause into his will that his estate should continue to operate his practice indefinitely after his death (the "Elvis" clause).
(e) Inserting a clause into his will that the files be securely shredded as soon as possible.

SCENARIO 3:

Andy is an OT working in the community home care setting. During the course of his day, Andy will often see upwards of ten clients. In order to ensure accurate documentation for each client, Andy carries each of his daily client charts in his vehicle during his work day. In order to ensure client privacy and confidentiality, Andy should:

(a) Read the files every morning before departing and leave the files at the office. He can then make notes as soon as he returns to the office.

© 2014, College of Occupational Therapists of Ontario

(b) Switch to electronic files and use a laptop computer with encryption.
(c) Store the files in a locked black case, the same colour as his car's floor mats, so that the case is barely visible from outside of the car.
(d) Carry all of the files in with him for every visit.
(e) Anonymize the files by using a number to identify his clients and locking the files in the trunk of his car.

SCENARIO 4:

Gwen, an OT, was hired by Sabrina, a private client in the community. Sabrina requested a workplace assessment as she was having difficulties meeting the demands of the workplace. Sabrina wanted to have a documented report with recommendations from an OT. Gwen completed the workplace assessment and indicated to her office administrator that the report was to go only to Sabrina. The office administrator did not have Sabrina's private contact information in the client file. The office administrator sent the report to Sabrina by fax to the general fax number at work. The cover sheet had a "confidentiality" statement on it. Sabrina was concerned that others at her place of work had access to the report. How should Gwen respond?

(a) Explain to Sabrina that the fax had a cover sheet with a confidentiality statement on it so that it was a secure transmission.
(b) Apologize to Sabrina, take steps to ensure there is no further access to the report and change her procedures so that mistakes like this do not happen again.
(c) Contact Sabrina's employer and ensure that the memory on the fax machine is securely wiped so that no one else can obtain access to the report.
(d) Apologize to Sabrina and transfer her care to another OT in whom Sabrina has confidence.
(e) Revise office procedures so that a form has to be filled out by the OT specifying precisely how reports are to be transmitted to avoid similar situations and then to tell Sabrina about the improvements.

SCENARIO 5:

Marthe, an OT, is social media-friendly. One day, Marthe receives a tweet from her colleague, Jun, a physiotherapist at their hospital. Jun reports completing a fundraising marathon with Cory and Jory, cognitively impaired young clients that both Marthe and Jun have worked with. The tweet refers to Cory and Jory as examples of what makes Jun's career meaningful. Marthe then checks Jun's Facebook page and notices pictures of Jun, Cory and Jory celebrating at the finish line. What should Marthe do?

(a) Report Jun to the hospital's privacy officer for disclosing personal health information about clients. Anyone reading both the tweet and the Facebook page would be able to determine that Cory and Jory were clients.
(b) Nothing, because no one reading the tweet by itself or the Facebook page itself would be able to identify the clients.
(c) Nothing, because Marthe has done nothing wrong and there are not any mandatory reporting obligations that apply to this situation.
(d) Speak with Jun about the privacy implications of his actions and suggest that Jun remove the pictures from his Facebook page.
(e) Speak with Jun generally about the need to be careful in his use of social media.

© 2014, College of Occupational Therapists of Ontario

SCENARIO 6:

Veronika, a solo-practising OT in the community has a twenty year-old client, Maggie, who is recovering from a motor vehicle accident. Maggie, while somewhat immature and dependent for her age, is capable of making decisions regarding her care and personal health information. Veronika faces the following requests for disclosure of Maggie's personal health information. Which request can be honoured without consulting Maggie?

(a) Maggie's employer asks for a return-to-work plan. Veronika believes that this disclosure to Maggie's employer would be in Maggie's best interests.
(b) Maggie's speech-language pathologist (SLP), who is also treating Maggie, asks for a copy of Veronika's chart. Maggie, for unknown reasons, does not agree to this request.
(c) Maggie's mother asks Veronika for information about Maggie's school plans.
(d) The insurer asks for additional information to help evaluate Maggie's entitlement to future care benefits.
(e) The College asks for Maggie's file to help with an investigation of another OT.

SCENARIO 7:

Upeksha, an OT, is working in a public hospital setting with patients who have had a cerebral vascular accident (CVA). One of her patients, Theodore, is being discharged to return home today. He is capable of making decisions about his care. Upeksha has to determine to whom she can disclose information without first contacting Theodore:

(a) The community PSW, to whom the patient is referred with regards to functional mobility and transfer safety within the home.
(b) Theodore's uncle, who is a lawyer managing Theodore's affairs through a power of attorney for property.
(c) Any registered health professional working at the hospital.
(d) Theodore's daughter, who will be helping with Theodore's care at home.
(e) The health supply company representative, who will be providing Theodore with a walker.

SCENARIO 8:

Safiyyah is an OT working in the community, performing assessments with elderly and disabled clients in their homes. Which of the following information about her clients would **not** be considered "personal health information" under PHIPA?

(a) The fact sheet she hands out to clients during flu season about preventing colds and the flu and the importance of immunization.
(b) Which daughter of a specific client is the client's substitute decision-maker.
(c) A client's health care number.
(d) A statement that Safiyyah is visiting every client on the third floor of the senior's apartment building.
(e) That a client is eligible for funding for assistive devices.

© 2014, College of Occupational Therapists of Ontario

SCENARIO 9:

Ray, an OT, is an excellent public speaker and has developed a sideline providing seminars and workshops for caregivers of children with autism. Ray provides strategies for navigating the government and school support systems, and valuable tips on how to cope with the stress and anxiety of being a caregiver to an autistic child. Almost half of Ray's income comes from these activities. Which of the following should Ray **not** do?

(a) Develop written policies and procedures for the collection, use and disclosure of personal information (e.g., names, addresses and credit card numbers of seminar and workshop attendees).
(b) Explain the reason why the personal information is being collected on his seminar and workshop registration forms.
(c) Collect only as much personal information as is necessary for Ray to offer the seminars and workshops.
(d) Ensure that, if any of the people attending a seminar or workshop are family members of his clients, he makes a note in the clients' clinical records of their attendance so he knows what they have been told.
(e) Safeguard the personal information through the same sorts of measures he uses for his clinical records (e.g., lock and key, password protection, etc.).

SCENARIO 10:

Rueben, an OT working in the community in a rehabilitation clinic, is working with Lucinda, a client who was in a motor vehicle accident and presents with cognitive impairments. Lucinda's lawyer has asked for a report on the impact of the accident on Lucinda's functional abilities to use in a court case. There is no way that Lucinda would understand this request and give Rueben informed consent. Lucinda's family is in conflict with one another and each of the following would want to be the substitute decision-maker. Assuming all of the following are available and capable, which one should Rueben obtain instructions from?

(a) Lucinda's husband of twenty years.
(b) Lucinda's eldest daughter.
(c) Lucinda's son, who has the power of attorney for property that includes decisions about personal health information.
(d) Lucinda's mother.
(e) Lucinda's sister, who has been appointed by the Consent and Capacity Board to give consent for OT treatment.

© 2014, College of Occupational Therapists of Ontario

APPENDIX A

Glossary

Agent: an individual who is authorized to perform services or activities on behalf of a health information custodian.

Client: (also referred to as "the patient" in the RHPA) is the individual (or group of individuals) or the client's authorized representative, whose occupational performance issue(s) is (are) the focus of care.

Circle of Care: a non-defined term under the *Personal Health Information Protection Act* (PHIPA, 2004) used to describe Health Information Custodians and their authorized agents who are permitted to rely on an individual's implied consent when collecting, using, disclosing, or handling personal health information for the purpose of providing direct health care.

Confidentiality: the obligation a healthcare provider/agency has to ensure the client's right to privacy is respected by limiting the access to, or improper use of information without the client's authorization.

Custodian: (also referred to as the Health Information Custodian), is a listed individual or organization under PHIPA that, as a result of his/her or its power or duties, has custody or control of personal health information.

Encryption: is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Estate: in the context of a death of an individual, the assets and liabilities of the deceased person that must be managed by a personal representative, so that any remaining assets can be distributed to the deceased person's beneficiaries.

FIPPA: *Freedom of Information and Protection of Privacy Act*, an Ontario statute dealing with the safeguarding of personal information and providing public access to government information and information held by representatives of the government. The Municipal *Freedom of Information and Protection of Privacy Act* is a parallel Ontario statute dealing with municipally-held information.

Firewall: a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

IPC: Information and Privacy Commissioner, an individual independent of the government who oversees privacy-related statutes in Ontario, including PHIPA and FIPPA.

Lock Box: a non-defined term under the *Personal Health Information Protection Act* (PHIPA, 2004), used to describe the right of an individual to instruct a health information custodian not to disclose specified personal health information to another custodian for the purpose of providing health care. An individual can be said to have placed his/her personal health information into a lock-box by expressly withholding or withdrawing consent for his/her health information to be collected, used or disclosed.

© 2014, College of Occupational Therapists of Ontario

Personal Health Information: personal information related to an individual's health and health care as defined in the *Personal Health Information Protection Act* (PHIPA, 2004).

Personal Information: information about an identifiable individual, which includes, but is not limited to, personal health information, but which excludes the name, business title or business address and telephone number of an individual.

PHIPA: *Personal Health Information Protection Act*, an Ontario statute dealing with the collection, use and disclosure of personal health information.

PIPEDA: *Personal Information and Protection of Electronic Documents Act*, a Canadian statute that protects the collection, use and disclosure of personal health information for commercial purposes. Since Ontario has PHIPA, it does not apply to personal health information in Ontario, but continues to apply to non-health personal information used for commercial purposes in Ontario.

Privacy: the right individuals have to control how their personal information is handled, that is, their right to determine what personal information is collected, used and disclosed, when, how and by whom.

Statute: an enactment (i.e. an Act) made by the Legislative Assembly of Ontario or the Parliament of Canada.

© 2014, College of Occupational Therapists of Ontario

APPENDIX B

Best Responses – Reflective Practice Exercise

The Prescribed Regulatory Education Program (PREP) is designed to help you stay up-to-date in your professional practice. The College developed this module to assist Registrants in understanding and complying with their professional obligations regarding confidentiality and privacy.

PREP modules are self-directed learning tools for adult learners. Reading and reflecting on the answers and rationale reinforces learning and may help you identify further learning needs. Registrants confirm that most learning occurs from engaging in the process of completing a module. Reviewing the answers and rationale with other OTs can enhance your learning experience. It is a professional responsibility to take action if you identify a learning need. You are encouraged to incorporate your identified learning needs in your Professional Development Plan.

The practice scenarios are brief and provide only key information. You may make assumptions that are different from those of the College so arrive at a different answer. What is important is that your understanding and rationale are sound. While not all choices are wrong, there is one or more best or most complete answers based on the information provided and the assumptions the College made.
If you identify that your reasoning is not sound or that you do not fully understand the material, record the actions you need to take to address the learning need in your Professional Development Plan.
Below are brief scenario summaries, please refer to section 10 for the complete situations.

SCENARIO 1:

Dero, an OT, operates a private practice. Which of the following is his responsibility as the custodian under the *Personal Health Information Protection Act* (PHIPA)?

(a) Hiring an outside person as Information or Privacy Officer.
(b) Creating and implementing a privacy policy for an organization.
(c) Reporting to the Information and Privacy Commissioner whenever a new staff person is hired.
(d) Creating and implementing a workplace violence policy for an organization.
(e) Ensuring that the filing cabinets are locked before he goes home.

The best answer is (b). A health information custodian is generally responsible for all health records retained by an organization, and must establish a privacy policy that governs the collection, use, disclosure and access to personal health information.

Answer (a) is not the best answer because the Information or Privacy Officer can be (and usually is) the OT or someone else from within the clinic or organization. The Information or Privacy Officer need not be from outside the organization.

Answer (c) is not the best answer because reporting the hiring of new staff is not an obligation under PHIPA. The Information and Privacy Commissioner monitors compliance with PHIPA and investigates complaints or concerns about non-compliance with the legislation.

© 2014, College of Occupational Therapists of Ontario

Answer (d) is not the best answer because PHIPA does not deal with workplace violence; it deals with privacy of personal health information. However, Dero probably requires a workplace violence policy under occupational health and safety legislation.

Answer (e) is not the best answer because it only covers a small portion of Dero's responsibility as the health information custodian. Locking filing cabinets is only a small portion of the broader duty to safeguard personal health information, which constitutes only a small portion of the custodian's overall responsibilities.

SCENARIO 2:

Dero (from Scenario 1) goes with his spouse to make a will. Which of the following options best respects his confidentiality and privacy obligations?

(a) Inserting into his will a clause that the College should be notified of his death and be asked to ensure that his client files are transferred to another OT.
(b) Inserting into his will a clause that the OTs at his practice at the time should divide the client files among themselves.
(c) Inserting into his will a clause that his estate takes custody of his files and makes arrangements to transfer them to another OT willing to take responsibility for his practice.
(d) Inserting a clause into his will that his estate should continue to operate his practice indefinitely after his death (the "Elvis" clause).
(e) Inserting a clause into his will that the files be securely shredded as soon as possible.

Answer (c) is the best answer because it establishes immediate authority and responsibility for the files and a reasonable process for ensuring that the personal health information is transferred to a suitable and willing custodian. Clients need to be told about the change of ownership and, if the files are moved, their new location.

Answer (a) is not the best answer because the College is a regulatory body and has no role in the custody and transfer of client files.

Answer (b) is not the best answer because there is no assurance that there will be OTs practising with him at the time of Dero's death, nor is there any assurance that they would be willing to assume responsibility for the files.

Answer (d) is not the best answer because estates are not registered with the College to practise occupational therapy, and often have no expertise in doing so. In addition, estates are generally intended to manage operations for only a short time, until a long-term solution can be found.

Answer (e) is not the best answer because privacy principles require that client files be retained for a reasonable period (generally ten years from the last contact or ten years after the client turned eighteen), therefore destroying the files immediately after the Dero's death is not the best option.

© 2014, College of Occupational Therapists of Ontario

SCENARIO 3:

Andy is an OT working in the community home care setting. In order to ensure client privacy and confidentiality, Andy should:

(a) Read the files every morning before departing and leave the files at the office. He can then make notes as soon as he returns to the office.
(b) Switch to electronic files and use a laptop computer with encryption.
(c) Store the files in a locked black case, the same colour as his car's floor mats, so that the case is barely visible from outside of the car.
(d) Carry all of the files in with him for every visit.
(e) Anonymize the files by using a number to identify his clients and locking the files in the trunk of his car.

The best answer is (e). It is always a challenge to safeguard files when making visits in the community. This question calls for reducing the risk to the lowest reasonable level. Depending on the circumstances, variations of some of the other answers might also be appropriate. Given the nature of Andy's practise, anonymizing paper files from the start may be the most practical. Andy would probably have to carry, perhaps in his pocket, a separate paper with the client's name, address and last few digits of the file number with him, but that would reduce the risk of a security breach greatly.

Answer (a) is not the best answer because it will compromise client care. Andy will not be able to remember all of the details nor will he be able to refer to the files during each visit.

Answer (b) is not the best answer because it is unreasonable to require Andy to switch from a paper format to an electronic format simply because he does home visits. If Andy is otherwise interested in switching formats, this option may make sense. However, there are security challenges with electronic records as well, even with encryption.

Answer (c) is not the best answer because the level of security is quite low. Passersby may, in fact, be attracted to the black case because of the ineffectual attempt to conceal it.

Answer (d) is not the best answer as the question reads now because the potential to misplace or forget the files is too high. Even if the files are maintained in a case that one is unlikely to forget, one will often leave the case unattended at some point during the visit. However, in some circumstances answer (d) could be the best answer. For example, if it was impossible to anonymize the files (e.g., because of the protocols where Andy worked) then an argument could be made that taking the files into the visit might be safer, particularly if other measures were taken (e.g., the case was locked; Andy put his car keys into the case so that it was impossible for him to leave without the case; Andy minimized the portions of the files brought with him; Andy developed a routine of never leaving the room without his case). The goal is always to reduce the risk to the lowest reasonable level.

SCENARIO 4:

Gwen, an OT, was hired by Sabrina, a private client in the community. Sabrina requested a work-place assessment as she was having difficulties meeting the demands of the workplace. The office

© 2014, College of Occupational Therapists of Ontario

administrator sent the report to Sabrina by fax to the general fax number at work. Sabrina was concerned that others at her place of work had access to the report. How should Gwen respond?

(a) Explain to Sabrina that the fax had a cover sheet with a confidentiality statement on it so that it was a secure transmission.
(b) Apologize to Sabrina, take steps to ensure there is no further access to the report and change her procedures so that mistakes like this do not happen again.
(c) Contact Sabrina's employer and ensure that the memory on the fax machine is securely wiped so that no one else can obtain access to the report.
(d) Apologize to Sabrina and transfer her care to another OT in whom Sabrina has confidence.
(e) Revise office procedures so that a form has to be filled out by the OT specifying precisely how reports are to be transmitted to avoid similar situations and then to tell Sabrina about the improvements.

The best answer is (b) because it covers all of the components of a good response to a privacy breach. Individuals whose personal health information has been compromised need to be advised (in this case, Sabrina already knew), likely with an apology. Immediate steps should be taken to contain the breach as much as is possible. Then the custodian's privacy policies should be revised to prevent similar occurrences in the future.

Answer (a) is not the best answer because there was a privacy breach. Other people had actual access to sensitive personal information. A confidentiality statement on the cover sheet of the fax is helpful, but not sufficient on its own.

Answer (c) is not the best answer because it only addresses one aspect of dealing with a privacy breach, trying to contain it. In addition, it is unlikely that the employer would be willing to wipe out the fax machine's entire memory in these circumstances. Thus, the response is unlikely to be helpful and may only draw the employer's attention to the privacy breach. This response highlights the challenges of containing an electronic privacy breach.

Answer (d) is not the best answer because it does not address the privacy breach. It simply ends the clinical relationship. It may be that Sabrina is still prepared to work with Gwen if Gwen acknowledges the error and addresses is appropriately.

Answer (e) is not the best answer because it only addresses one aspect of responding to a privacy breach. Changing policies when the previous ones have failed is appropriate, but is not sufficient in itself.

SCENARIO 5:

Marthe, an OT, receives a tweet from her colleague, Jun, a physiotherapist at their hospital. Marthe questions if Jun has inadvertently breeched client confidentiality through use of social media. What should Marthe do?

(a) Report Jun to the hospital's privacy officer for disclosing personal health information about clients. Anyone reading both the tweet and the Facebook page would be able to determine that Cory and Jory were clients.

© 2014, College of Occupational Therapists of Ontario

(b) Nothing, because no one reading the tweet by itself or the Facebook page itself would be able to qidentify the clients.
(c) Nothing, because Marthe has done nothing wrong and there are not any mandatory reporting obligations that apply to this situation.
(d) Speak with Jun about the privacy implications of his actions and suggest that Jun remove the pictures from his Facebook page.
(e) Speak with Jun generally about the need to be careful in his use of social media.

The best answer is (d) because it is a proportional response to a potential privacy breach. It may be that Jun has the consent of the clients to their inclusion in social media (although, even then, there may be issues about the voluntariness and informed nature of the consent).

Answer (a) is not the best answer because it is a disproportionate first response to the situation. This option may become appropriate if Jun does not respond appropriately to the concerns or continues his conduct. This option may also become appropriate if Marthe has a contractual obligation to the hospital to report any potential privacy breach.

Answer (b) is not the best answer because disclosure of personal health information can occur through the combination of two or more sources of information. That fact that one source by itself may not contain personal health information is not a complete answer. In addition, technically, the first names of the clients were revealed in the tweet.

Answer (c) is not the best answer because it does not address Marthe's ethical obligations under the circumstances. While the answer is accurate as far as it goes, it does not respect the privacy interests of Cory and Jory, and potentially, future clients.

Answer (e) is not the best answer because it does not address the existing social media postings about Cory and Jory.

SCENARIO 6:

Veronika, a solo-practising OT in the community has a twenty year-old client, Maggie, who is recovering from a motor vehicle accident. Veronika faces the following requests for disclosure of Maggie's personal health information. Which request can be honoured without consulting Maggie?

(a) Maggie's employer asks for a return-to-work plan. Veronika believes that this disclosure to Maggie's employer would be in Maggie's best interests.
(b) Maggie's speech-language pathologist (SLP), who is also treating Maggie, asks for a copy of Veronika's chart. Maggie, for unknown reasons, does not agree to this request.
(c) Maggie's mother asks Veronika for information about Maggie's school plans.
(d) The insurer asks for additional information to help evaluate Maggie's entitlement to future care benefits.
(e) The College asks for Maggie's file to help with an investigation of another OT.

Answer (e) is the best answer because it does not raise any concerns. Disclosure of personal health

© 2014, College of Occupational Therapists of Ontario

information to the College is expressly permitted under PHIPA without the client's consent. Such disclosure is necessary to make the regulatory system effective. In addition, there is a general legal and ethical obligation for OTs to cooperate with College investigations.

Answer (a) is not the best answer because this disclosure decision is up to the client and not the OT. The fact that the OT agrees with the disclosure decision is irrelevant. If Maggie authorizes the disclosure, the OT should make it, unless one of the exceptions applies (e.g., risk of harm).

Answer (b) is not the best answer because while the circle of care concept permits disclosure to others on the client's health care team, an exception is where the client expressly directs that the information not be disclosed. This is called the lock box concept. In the scenario, Maggie does not want the disclosure to be made. If Veronika believes that the speech-language pathologist requires the information to provide care, Veronika should tell the SLP that relevant information is being withheld from the file. It would also be appropriate for Veronika to discuss Maggie's concerns with her to see if they can be addressed.

Answer (c) is not the best answer because when a client is capable of deciding what happens to his or her personal health information, disclosure should not happen, even to the client's parent, unless the client consents or one of the exceptions applies (e.g., risk of harm). Here, there is no information to suggest that Maggie has consented to the disclosure. Consent will likely be easy to obtain, but must be sought first.

Answer (d) is not the best answer because there is no information to suggest that Maggie has consented to the disclosure. Expressed consent is required for disclosure to third parties who are not providing health care.

SCENARIO 7:

Upeksha, an OT, is working in a public hospital setting with patients who have had a cerebral vascular accident (CVA). Upeksha has to determine to whom she can disclose information without first contacting the client, Theodore:

(a) The community PSW, to whom the patient is referred with regards to functional mobility and transfer safety within the home.
(b) Theodore's uncle, who is a lawyer managing Theodore's affairs through a power of attorney for property.
(c) Any registered health professional working at the hospital.
(d) Theodore's daughter, who will be helping with Theodore's care at home.
(e) The health supply company representative, who will be providing Theodore with a walker.

The best answer is (a) because the PSW is a health care worker who is becoming involved in Theodore's care. There is implied consent to discuss Theodore's care with others on the health care team for the purpose of advancing Theodore's care unless Theodore invokes the lockbox. Of course, Upeksha should always consider discussing such disclosure with Theodore first when this is feasible, or when Upeksha believes Theodore might be surprised at the disclosure.

© 2014, College of Occupational Therapists of Ontario

Answer (b) is not the best answer because a family member is not part of the circle of care. A power of attorney over property may be a suitable substitute decision-maker with respect to access to and disclosure of personal health information if Theodore is incapable or if the power of attorney specifically applies to personal health information while Theodore is capable. But that is a different concept from the circle of care.

Answer (c) is not the best answer because not every health professional at a hospital will be involved in Theodore's care. The circle of care includes only those actually involved in health care delivery to the patient.

Answer (d) is not the best answer because a family member is not part of the circle of care, even if that family member helps take care of the client. Consent is needed to disclose personal health information to Theodore's daughter.

Answer (e) is not the best answer because the supplier of health products is not a health care practitioner. Consent is needed to disclose Theodore's personal health information to the supplier.

SCENARIO 8:

Safiyyah is an OT working in the community, performing assessments with elderly and disabled clients in their homes. Which of the following information about her clients would not be considered "personal health information" under PHIPA?

(a) The fact sheet she hands out to clients during flu season about preventing colds and the flu and the importance of immunization.
(b) Which daughter of a specific client is the client's substitute decision-maker.
(c) A client's health care number.
(d) A statement that Safiyyah is visiting every client on the third floor of the senior's apartment building.
(e) That a client is eligible for funding for assistive devices.

The best answer is (a) because it does not identify any specific client. However, even this would become personal health information if Safiyyah identified which clients she gave the fact sheet to, because then she would be identifying specific advice given to specific clients.

Answer (b) is not the best answer because the identity of a substitute decision-maker is information related to the health and care of the client, and is therefore defined in PHIPA as personal health information.

Answer (c) is not the best answer because the health care number of a client is information related to the health and care of the client, and is therefore defined in PHIPA as personal health information.

Answer (d) is not the best answer because this would identify Safiyyah's clients to anyone who knew which residents lived on the third floor of the building.

© 2014, College of Occupational Therapists of Ontario

Answer (e) is not the best answer because eligibility for funding is information related to the health and care of the client, and is therefore defined in PHIPA as personal health information.

SCENARIO 9:

Ray, an OT, is an excellent public speaker and has developed a sideline providing seminars and workshops for caregivers of children with autism. Which of the following should Ray NOT do?

(a) Develop written policies and procedures for the collection, use and disclosure of personal information (e.g., names, addresses and credit card numbers of seminar and workshop attendees).
(b) Explain the reason why the personal information is being collected on his seminar and workshop registration forms.
(c) Collect only as much personal information as is necessary for Ray to offer the seminars and workshops.
(d) Ensure that, if any of the people attending a seminar or workshop are family members of his clients, he makes a note in the clients' clinical records of their attendance so he knows what they have been told.
(e) Safeguard the personal information through the same sorts of measures he uses for his clinical records (e.g., lock and key, password protection, etc.).

The best answer is (d) because neither PHIPA nor PIPEDA requires the integration of information in this manner. In addition, attendees of the seminars and workshops should know how their information is being used, so transferring this information to the clients' clinical records would violate the attendees' privacy rights, unless they were informed of this ahead of time (and had the option of refusing). However, where this information is relevant for the care of the clients, the OT might add this information to the relevant clinical records with the consent of the seminar and workshop attendees.

Answer (a) is not the best answer because developing written privacy policies is a requirement under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA applies to any commercial activity (which would include workshops and seminars for profit) that is not covered by PHIPA (i.e., PHIPA deals with the provision of health care). The requirements of PIPEDA are quite similar to those of PHIPA, as they are based on the same privacy principles. Customers have many of the same rights of control over their personal information as do clients under PHIPA.

Answer (b) is not the best answer because explaining why personal information is collected is a requirement under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA applies to any commercial activity (which would include workshops and seminars for profit) that is not covered by PHIPA (i.e., PHIPA deals with the provision of health care).

Answer (c) is not the best answer because limiting the collection of personal information to what is necessary for the purpose is a requirement under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Answer (e) is not the best answer because safeguarding personal information is a requirement under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

© 2014, College of Occupational Therapists of Ontario

SCENARIO 10:

Rueben, an OT working in the community in a rehabilitation clinic, is working with Lucinda, a client who was in a motor vehicle accident and presents with cognitive impairments. Lucinda's lawyer has asked for a report on the impact of the accident on Lucinda's functional abilities to use in a court case. Assuming all of the following are available and capable, which one should Rueben obtain instructions from?

(a) Lucinda's husband of twenty years.
(b) Lucinda's eldest daughter.
(c) Lucinda's son, who has the power of attorney for property that includes decisions about personal health information.
(d) Lucinda's mother.
(e) Lucinda's sister, who has been appointed by the Consent and Capacity Board to give consent for OT treatment.

The best answer is (c) because on the ranking of substitute decision-makers, powers of attorney come second, just behind a court-appointed guardian (which does not exist in this scenario). Since all of those listed are capable, available and willing, the highest-ranked substitute will make the decision. In a situation this complex and fraught with conflict, Rueben may wish to obtain advice.

Answer (a) is not the best answer because the client's spouse is ranked lower than the power of attorney for property that includes decisions about personal health information. In a situation this complex and fraught with conflict, Rueben may wish to obtain advice.

Answer (b) is not the best answer because the client's child is ranked lower than the power of attorney for property that includes decisions about personal health information. In a situation this complex and fraught with conflict, Rueben may wish to obtain his own legal advice.

Answer (d) is not the best answer because the client's parent is ranked lower than the power of attorney for property that includes decisions about personal health information. In a situation this complex and fraught with conflict, Rueben may wish to obtain advice.

Answer (e) is not the best answer because the client's representative appointed by the Consent and Capacity Board is ranked lower than the power of attorney for property that includes decisions about personal health information. This is one of those rare occasions where the substitute authorized to give consent for treatment is different than the substitute who is authorized to give consent for the collection, use and disclosure of personal health information. In a situation this complex and fraught with conflict, Rueben may wish to obtain advice.

© 2014, College of Occupational Therapists of Ontario

APPENDIX C

References

Checklist for Health Information Custodians in the Event of a Planned or Unforeseen Change in Practice (Information and Privacy Commissioner, May 29, 2007), found at **www.ipc.on.ca**.

Circle of Care: Sharing Personal Health Information for Health-Care Purposes, (Information and Privacy Commissioner of Ontario, September 2, 2009), found at **www.ipc.on.ca**.

Code of Ethics – Commitment to Good Practice, (College of Occupational Therapists of Ontario, 2011), found at **www.coto.org**.

Conscious Decision-Making in Occupational Therapy, (College of Occupational Therapists of Ontario, September 2012), found at **www.coto.org**.

Decisions and Resolutions, (Information and Privacy Commissioner of Ontario, various dates), found at **www.ipc.on.ca**.

Essential Competencies of Practice for Occupational Therapists in Canada, 3rd Edition (College of Occupational Therapists of Ontario, May 2011), found at **www.coto.org**.

Fact Sheet #12 - Encrypting Personal Health Information on Mobile Devices, (Information and Privacy Commissioner of Ontario, May 1, 2007), found at **www.ipc.on.ca**.

Guide to the Code of Ethics, (College of Occupational Therapists of Ontario, June 2012), found at **www.coto.org**.

Guideline: Use of Surveillance Material in Assessment, (College of Occupational Therapists of Ontario, November 2012), found at: www.coto.org.

Jones v. Tsige, 2012 ONCA 32, found at **www.canlii.org**.

McInerney v. MacDonald, [1992] 2 S.C.R. 138, found at **www.canlii.org**.

Nursing 2.0, (Ontario College of Nurses of Ontario, (*The Standard*, Fall 2011, Volume 36, Issue 3), found at **www.cno.org**.

Occupational Therapy Professional Misconduct Regulation, Ontario Regulation 95/07, found at **www.e-laws.gov.on.ca**.

Personal Health Information Protection Act (2004), Statutes of Ontario, 2004, c. 3, Schedule A, found at **www.e-laws.gov.on.ca**.

© 2014, College of Occupational Therapists of Ontario

Professional Advisory – Use of Electronic Communication and Social Media, (Ontario College of Teachers, February 23, 2011), found at **www.oct.ca**.

Social Media in OT Practice, Lily Wainer, (*On the Record*, Fall 2011, Volume 11, Issue 3), found at **www.coto.org**.

Standards for Record Keeping, (College of Occupational Therapists of Ontario, 2008), found at **www.coto.org**.

© 2014, College of Occupational Therapists of Ontario