ONA MEMBERS AND PATIENT PRIVACY: BE AWARE AND BEWARE!

Adapted from a presentation by ONA General Counsel Elizabeth J. McIntyre, Cavalluzzo Shilton McIntyre Cornish LLP, ONA Provincial Coordinators Meeting, June 2015

The headlines were frightening.

► “Nurse suspended for snooping into files.” — Toronto Star, May 2015

► “Health ‘snooping’ cases on the rise; Privacy commissioner repeats request that charges be laid against violators” — Toronto Star, May 2015

► “5 people accused of criminal and securities offences over sale of new mothers’ confidential records” — CBC News, June 2015

► “Massive privacy breach at a Toronto hospital has led to 19 more charges, including six criminal counts against a nurse…” — CBC News, June 2015

ONA General Counsel Liz McIntyre made a presentation to ONA leaders on patient privacy issues at the June 2015 Provincial Coordinators Meeting.
On November 1, 2004, the Personal Health Information and Protection Act (PHIPA) came into force. The purpose of the law is twofold:
- Establishes rules for the collection, use and disclosures of personal health information (PHI).
- Protects the confidentiality of individuals while facilitating the effective provision of health care.

A recent rash of stories in the media about privacy breaches, many referencing nurses, has put this legislation back in the spotlight and has legislators looking at amendments to toughen up the laws. (See story, “Ontario’s Privacy Laws Undergoing Revisions,” page 3.)

In a presentation to ONA leaders at the June 2015 Provincial Coordinators Meeting (PCM), ONA General Counsel Liz McIntyre said members should **BE AWARE** of privacy laws around PHI, and **BEWARE** how they access and use PHI.

“Where complaints have been made, there has been an overreaction from the media and, unfortunately, some health care professionals have been caught in it,” McIntyre said.

“The focus is on the circle of care, and if you are not in that circle, you are considered to be snooping. Some have violated PHIs for their own purposes, but it’s more often that the training of health care professionals by employers has been inadequate, and there are unclear rules of what is and isn’t permitted. Practices in hospitals are inconsistent and employers need to make sure everyone is educated.”

The “circle of care” refers to the health care providers who work as a team to provide care and make decisions.

### Who does PHIPA apply to?

PHIPA applies to health information custodians, institutions and health care practitioners and agents or employees of a custodian.

Health information custodians are assigned primary responsibility for PHI and must take steps to ensure the confidentiality and privacy of PHI. These include hospitals, long-term care homes, nursing homes, community care access centres, medical laboratories, pharmacies and community health programs, as well as health care practitioners who operate institutions.

Health care practitioners are identified as regulated health care providers under the Regulated Health Professions Act (RHPA). They are considered “agents,” and they have the same duties and obligations of confidentiality as agents of custodians.

### Tips to Safeguard Your Practice

- Ensure that your employer has up to date and clear policies.
- Know what the rules are.
- Insist on ongoing education on policies.
- Log out when not using your computer.
- Change your password.
- Do not release information to the police or other third parties.
- Refer police/third parties to a supervisor or medical records department.
- Remember that the definition of PHI is very broad.
- Be aware of the audit capabilities of computers.
- Report accidental access to management.
What does the Act apply to?

PHI may be oral or in recorded form. It is information that:

- Relates to the physical or mental health of the individual.
- Relates to the health care provided.
- Identification of a health provider or a substitute decision-maker of the individual.
- Eligibility of health care coverage or coverage for health care in respect of an individual.
- Health number of an individual.

Ontario’s Privacy Laws Undergoing Revisions

On September 16, 2015, the Ontario government announced it plans to introduce legislation intended to improve privacy, accountability and transparency in the health-care system.

Bill 119, the Health Information Protection Act, 2015 (HIPA), amends existing legislation – the Personal Health Information Protection Act, 2004 (PHIPA) and the Quality of Care Information Protection Act, 2004 (QCIPA) – to protect the personal health information of patients.

Amendments to PHIPA include:

- Making it mandatory to report privacy breaches, as defined in the regulation, to Ontario’s Information and Privacy Commissioner and to relevant regulatory colleges.
- Strengthening the process to prosecute offences under PHIPA by removing the requirement that prosecutions must commence within six months of the alleged offence.
- Doubling the maximum fines for offences from $50,000 to $100,000 for individuals and $250,000 to $500,000 for organizations.

HIPA also updates QCIPA to help increase transparency and maintain quality in Ontario’s health-care system.

If passed, this new bill, which has received first reading in the legislature, would:

- Affirm the rights of patients to access information about their own health care.
- Clarify that certain information and facts about critical incidents cannot be withheld from affected patients and their families.
- Require the Minister of Health and Long-Term Care to review QCIPA every five years.

An employee must notify the employer as soon as possible if information under their control is lost, stolen, used or disclosed without authority. If an employee doesn’t comply with any conditions or restrictions imposed by their employer under the legislation, he or she might be in breach of the Act and subject to the penalties under the Act as well as employer discipline.

The employer is required to advise a regulatory health college if it terminates, suspends or disciplines one of its employees as a result of inappropriate use, disclosure, retention, etc., of PHI or if the member resigns and if there are reasonable grounds to believe the resignation is related to an investigation regarding the above.

There would be no limitation period for filing complaints pursuant to the Act (currently there is a six-month limitation period).
Collection, Use and Disclosure

Collection: To gather, acquire, receive or obtain PHI by any means from any source, directly from the patient or indirectly from a source other than the patient.

Use: To handle or deal with the information, but does not include disclosure of the information; the internal usage and transfer of information within an institution is "use" and not a disclosure.

Disclosure: To make PHI available to release to another custodian or person.

The law obliges custodians of PHI to have specific safeguards in place and develop practices which comply with requirements under PHIPA. Practices must be in writing and available to the public. They must have a contact person to facilitate compliance under the Act and they must ensure records are retained, transferred and disposed of in a secure manner.

Custodians/agents cannot collect disclose or use PHI without either the individual’s consent or as the Act permits. Consent means that a person knows the purpose of the collection, use or disclosure of their PHI.

Uses Permitted Under PHIPA (S. 37) Without Consent
- Providing care to the patient.
- Planning or delivering of programs or services.
- Risk/error management.
- Maintaining/improving quality of care.
- Educating agents to provide care.

Consequences of a Breach of the Duty of Confidentiality
- May be grounds for discipline up to and including termination.
- May also result in disciplinary action by the College of Nurses of Ontario (CNO) under the RHPA. In November 2004, the CNO revised its Standard of Practice on Confidentiality and Privacy to incorporate PHIPA.

A breach of the duty of confidentiality is very serious. McIntyre calls it “quadruple jeopardy:
1) Many employers have a zero tolerance policy and terminate.
2) The CNO may enact disciplinary action.
3) There is the possibility of civil liability and damages.
4) Willful or intentional contraventions are considered to be a provincial offence and may attract fines.

To safeguard your practice, McIntyre recommends that members:
- Ensure your employer has up-to-date and clear policies that you understand and insist on ongoing education on those policies.
- Log out when not using computers and change your password often.
- Be aware of the audit capabilities of computers.
- Do not release information to the police or other third parties and refer them instead to a supervisor or the medical records department.
- Report accidental access to management.

A series of questions and answers regarding access to PHI follows on the next few pages.
Access to Confidential Patient, Resident and/or Client Records

Questions & Answers

The confidentiality of medical information has been at the forefront of legislative changes in Ontario with the introduction of the **Personal Health Information Protection Act (PHIPA)** in 2004.

Health professionals have always been held to a high standard with respect to maintaining the confidentiality of patient, client and/or resident information. Many institutions, including hospitals, nursing homes, community care access centres (CCACs), health units and home care providers, have revamped their policies and procedures to address these changes.

ONA members need to be vigilant in your practice to maintain patient, resident and/or client confidentiality. Always log off your employer’s computer system to avoid others improperly accessing the system using your login. Members should avoid any and all improper access to medical information or risk severe discipline or termination for such breaches. Members should never allow another employee or physician to access patient records through their login.
What follows are sample questions and answers based largely on real fact scenarios involving ONA members.

**Q:** My daughter is in the hospital. Can I access her medical information on the hospital’s electronic system as I have legal consent to access her records?

**A:** No. Unless you are a member of your daughter’s health care team, you are not entitled to access her medical file on the hospital’s electronic system. If you have legal consent to receive her medical file, you must follow the proper process for obtaining that information. Accessing the information directly could result in discipline or termination of employment.¹

**Q:** I work in the Healthy Babies/Healthy Children program at a health unit. My neighbour’s daughter is a client in the program. My neighbour called me the other day asking whether her daughter had been regularly attending and actively participating in the program. Can I respond to her?

**A:** No. The client’s attendance and participation in the program is potentially health information as defined under PHIPA and cannot be disclosed without the client’s consent. The fact that the program itself may take place in a public setting with other clients present does not negate the obligation owed under the statute.

**Q:** I heard that our hospital does regular audits to see who is accessing patient records. Can they do this? Is this not a violation of my privacy rights as it tracks when I am logging on and off the system?

**A:** Hospitals are defined as health information custodians under PHIPA. Health information custodians have a legal obligation to maintain the confidentiality of patients’ health records. Where a hospital uses an electronic records system that provides access to various medical staff, it has an obligation to put safeguards in place. This may include regular audits of the electronic system to ensure that staff is not improperly accessing patient information. An employee does not have a right to privacy with respect to this type of monitoring.

**Q:** I accidentally logged into the medical records of patients who are not under my care. Should I report this to my manager?

**A:** Yes. Nurses can be disciplined or terminated for even minor breaches of patient confidentiality. Hospitals commonly do audits of their electronic medical systems to detect potential breaches. At least one arbitrator has stated that a nurse could not use a defense that she logged into a record by error when she failed to report that error to the hospital.² Keep a paper trail that you have informed your manager.

**Q:** My employer has no policies or procedures in place to address access to patient records. Can I get in trouble for accessing records when there are no policies in place?

**A:** Yes. The obligation to maintain patient confidentiality is established both under statute (PHIPA) and through professional standards regulated by the College of Nurses of Ontario (CNO).³ A nurse who breaches those standards and statutory obligation may be disciplined regardless of the absence of any internal policies or procedures.
Q: I work at a CCAC. Out of curiosity, I accessed numerous client files that were not my own client but were people in the community that I know. Does my employer have an obligation to notify those clients of this potential breach?
A: Yes. PHIPA specifically provides that health information custodians have an obligation to advise patients, clients or residents of any breach of their privacy rights.4

Q: Can I be sued for improperly accessing patient information?
A: Yes. The legislation (PHIPA) contemplates that members of the public can take legal action against both an institution and individuals who violate their rights under the Act.5 There is also now new legislation on this issue that permits a lawsuit.

Q: Can I access patient records for strictly learning purposes?
A: The answer will depend on whether you are part of the care team for these patients, or have authorization through a research study or through some other means. If you are part of the care team, (e.g. part of the Circle of Care) your right to access patient records is implied. If you are working as part of a research study, ensure that you have expressed written consent that confirms authorization to access patient records. If none of these apply, you cannot take it upon yourself to access patient records for learning purposes. Those who do so risk discipline or termination.6

Q: Can I access my own medical records (e.g. blood results) through the hospital’s electronic patient records?
A: No. Accessing your own records is not a breach of privacy under PHIPA or a breach of the CNO standards; however, it may be a violation of the employer’s policy, which can result in discipline.

Q: One of my coworkers was recently admitted to the hospital. I want to access her information on the electronic system just to see if she has been discharged or is still in the hospital. Can I access the system for this purpose only?
A: No. This is unauthorized access that could result in discipline or termination. The fact that you had no intent to access any medical information is irrelevant to the breach.

NOTES
1 ONA and Bluewater Health (W. Rayner, November 26, 2010)
2 See Bluewater Health supra
3 Professional Standard: Confidentiality of Privacy – Personal Health Information (College of Nurses of Ontario, 2008)
4 S. 16(2) PHIPA
5 S. 65 PHIPA
6 ONA and North Bay Health Centre (R. Abramsky, January 9, 2012)
Q: I sometimes forget to log off the computer system after reviewing my patient’s files. Can I get in trouble for this?

A: A nurse is responsible for logging on and off the system. If you do not log off, any other person can get onto the system and access other patient files. If the system is open under your name, it will appear as if you are the one improperly accessing files. The CNO Standard of Practice expressly states that nurses are responsible for “safeguarding the security of computerized, printed or electronically displayed or stored information against unauthorized access or use” and “should not share computer passwords.”7 If you are called away as a result of an emergency and did not log off, inform your employer immediately to ensure they are aware if files are accessed during your absence.

Q: A physician in the nursing home where I work can never remember his password. He is always asking the nurses to log into the system for him. Can these nurses get in trouble for this practice?

A: For the same reasons as stated above, a nurse should not be allowing other users to go into the system under her or his name. The electronic system cannot differentiate who is on the system, and the assumption will be it is the nurse who initially logged on.

Q: I just found out that my son-in-law was admitted to the emergency department. I am currently at work on a different unit and do not have time to go down to emergency. My son-in-law is allergic to certain medications. Can I go on the meditech system to ensure that staff has documented this?

A: No. You do not have authorization to access his records as you are not part of his health care team. You must follow the proper procedure and call down to the emergency department and advise them directly.8

NOTES
7 Confidentiality of Privacy – Personal Health Information supra
8 ONA and Timmins and District Hospital (W. Marcotte, May 11, 2011)