Reporting Privacy Breaches

Regulated health professionals in Ontario need to be aware of new reporting obligations under the *Personal Health Information Protection Act, 2004* (PHIPA).[1] These changes took effect in June 2016.

What is a privacy breach?

Under PHIPA, a privacy breach is considered to be the unauthorized use or disclosure of personal information or the loss or theft of personal health information. This includes the viewing of health records by someone who is not allowed to view those records (known as "snooping"). Other examples include where a USB key with health information goes missing or a briefcase with patient files is taken from someone's car.

Who needs to be notified?

If this occurs, the health information custodian (the person with custody and control of the records) needs to notify the affected individual at the first reasonable opportunity. The law now requires the health information custodian to also notify the individual that the individual can make a complaint about the breach to the Information and Privacy Commissioner of Ontario.

If you are an agent of a health information custodian (for example, if you are a regulated health professional that works for a group practice, a hospital or for another regulated health professional) you need to tell the responsible custodian at the first reasonable opportunity.

When new regulations are passed, health information custodians will also have to report certain privacy breaches to the Information and Privacy Commissioner directly. Until the regulations are passed, reporting to the Commissioner is not mandatory, but may be done voluntarily.

Reporting to Regulatory Colleges

The changes to PHIPA now also require health information custodians to report certain actions taken in response to privacy breaches to the appropriate regulatory College.

This means that if a health information custodian takes any disciplinary action against a member of a College under the *Regulated Health Professions Act, 1991* or the Ontario College of Social Workers and Social Service Workers because of that member's unauthorized collection, use, disclosure, retention or disposal of personal health information, the custodian must report that fact to the member's regulatory College. This includes situations where a custodian suspends or terminates a member's employment or revokes or restricts a member's privileges or business affiliation. It also includes situations where the member resigns in the face of such action.

[1] PHIPA was amended by the *Health Information Protection Act, 2016*, S.O. 2016, c. 6 (Bill 119).

This notice must be given within 30 days of the disciplinary action or resignation occurring and it must be in writing. Additional requirements or exceptions may be set out in a future regulation.

This new notice requirement under PHIPA overlaps with the mandatory reporting provisions of the *Regulated Health Professions Act, 1991*, which require employers to report when a member has been terminated or had their privileges or partnership revoked or restricted for reasons of professional misconduct, incompetence or incapacity. Given that each College defines professional misconduct differently, the purpose of the amendments to PHIPA is to make it clear that action taken in response to privacy breaches must be reported to the appropriate College.

Other Important Changes

In addition to the new reporting obligations, the following changes have also been made to PHIPA:

- The maximum fines for privacy offences have doubled from $50,000 to $100,000 for individuals and from $250,000 to $500,000 for organizations.
- The limitation period for prosecutions of privacy offences has been removed.
- The respective responsibilities of health information custodians and agents have been clarified.
- A framework for a province-wide system of electronic health records has been introduced, but is not yet in force.

A new *Quality of Care Information Protection Act, 2016* has also been passed, but is not yet in force.