Reporting Privacy Breaches:

Personal Health Information Protection Act Amendments

Registered Massage Therapists ('RMTs' / 'MTs') in Ontario need to be aware of new reporting obligations under the *Personal Health Information Protection Act, 2004* (PHIPA). Important changes took effect on October 1, 2017.

What is a privacy breach?

A privacy breach is when someone's personal health information is used or disclosed without authority or when their information is lost or stolen. Looking at a client's health records without authority – known as "snooping" – is considered to be a privacy breach. Other examples include where a USB key with health information goes missing, when a computer or smartphone that is used for storing client information or communicating with clients is lost, or a briefcase with client files is taken from someone's car.

Who is considered to be a Health Information Custodian (HIC) or an agent?

Individuals and organizations that deliver healthcare are health information custodians ("HICs") under PHIPA. HICs have certain legal responsibilities with respect to the collection, use and disclosure of the personal health information. As an RMT if you have custody and control of client health information in connection with your practice, then you are an HIC for the purposes of PHIPA. However, if you work for or on behalf of another HIC (such as another regulated health professional, a group practice or a hospital), then you are considered to be an 'agent' of that HIC. An HIC is ultimately responsible for the personal health information in his or her custody or control, but may permit an agent to collect, use, disclose, retain or dispose of the information if certain requirements are met. The agent must ensure that the collection, use, disclosure, retention or disposal of the information is permitted by the HIC, is necessary for purposes of carrying out the agent's duties, is not contrary to law and complies with any specific restrictions imposed by the HIC.

Who needs to be notified?

The Client

If a client's personal health information is stolen, lost, or used or disclosed without authority, the HIC (the person with custody and control of the records) needs to notify the client at the first reasonable opportunity. The HIC also has to tell the client that he or she can make a complaint about the breach to the Information and Privacy Commissioner (IPC) of Ontario.

The Health Information Custodian (HIC)

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

The Information and Privacy Commissioner of Ontario (IPC)

Effective **October 1, 2017**, HICs have to report the following types of privacy breaches to the IPC directly:

1. *Use or disclosure without authority:* The HIC has reasonable grounds to believe that personal health information in the custodian's custody or control was used or disclosed without authority by a person who knew or ought to have known that they were using or disclosing the information without authority.
2. *Stolen information:* The HIC has reasonable grounds to believe that personal health information in the custodian's custody or control was stolen.
3. *Further use or disclosure without authority:* The HIC has reasonable grounds to believe that, after an initial loss or unauthorized use or disclosure of personal health information in the custodian's custody or control, the personal health information was or will be further used or disclosed without authority.
4. *Pattern of similar breaches:* The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures of personal health information in the custody or control of the HIC.
5. *Disciplinary action taken against a registrant of regulatory College:* The HIC is required to give notice to a College of an event described in section 17.1 of PHIPA that relates to a loss or unauthorized use or disclosure of personal health information (discussed below).
6. *Disciplinary action taken against others:* The HIC would be required to give notice to a College, if an agent of the HIC were a registrant of the College, of an event described in section 17.1 of PHIPA that relates to a loss or unauthorized use or disclosure of personal health information.
7. *Significant breaches:* The HIC determines that the loss or unauthorized use or disclosure of personal health information is significant after considering all relevant circumstances, including the following:

    i. Whether the personal health information that was lost or used or disclosed without authority is sensitive.

    ii. Whether the loss or unauthorized use or disclosure involved a large volume of personal health information.

    iii. Whether the loss or unauthorized use or disclosure involved many individuals' personal health information.

    iv. Whether more than one HIC or agent was responsible for the loss or unauthorized use or disclosure of the personal health information.

Regulatory Colleges

HICs are also required to report certain actions taken in response to privacy breaches to the appropriate regulatory College. For example, if you fired an RMT because they had stolen client records, you would need to report this to the College of Massage Therapists of Ontario (CMTO).

Situations that need to be reported to a regulatory College include:

- If an HIC terminates, suspends or otherwise disciplines a registrant of a College because of a privacy breach;
- If an HIC revokes, suspends or restricts the privileges or business affiliation of a registrant of a College because of a privacy breach; and
- If the registrant of the College resigns in the face of such action.

The notice to the regulatory College must be given within thirty (30) days of the disciplinary action or resignation occurring and it must be in writing. As noted above, if a report is made to a College in one of these circumstances, then a report must also be made to the IPC.

This notice requirement under PHIPA overlaps with the mandatory reporting provisions of the *Regulated Health Professions Act, 1991*, which require employers to report when a registrant has been terminated or had their privileges or partnership revoked or restricted for reasons of professional misconduct, incompetence or incapacity.

Annual Report to the IPC

Starting in **January 2018**, HICs will have to start tracking information about privacy breaches that occur in their organizations. HICs will have to provide an annual report to the IPC about any privacy breaches starting in **March 2019**.

Conclusion

It is important for all RMTs to understand their obligations under PHIPA, including when they need to report privacy breaches and to whom those reports need to be made.

More information can be obtained on the IPC's website: https://www.ipc.on.ca/health/report-a-privacy-breach/

The full text of the new Regulation under PHIPA is available on e-Laws: https://www.ontario.ca/laws/regulation/040329