



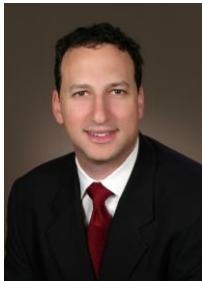
GARDINER ROBERTS LLP
Lawyers

Gardiner Roberts LLP

Barrister & Solicitors
Scotia Plaza
40 King St. West
Suite 3100
Toronto, ON
M5H 3Y2

Tel: 416-865-6600
Fax: 416-865-6636

www.gardiner-roberts.com



This article was prepared by Lonny Rosen. Mr. Rosen is a partner in our health law department and can be reached at 416-369-4345 or lrosen@gardiner-roberts.com

PRIVACY COMPLIANCE: ARE WE THERE YET?

This November, Ontario's health privacy legislation, the *Personal Health Information and Protection Act, 2004* (PHIPA) will have been in force for four years. PHIPA governs the manner in which personal health information is to be collected, used and disclosed by health information custodians, such as mental health agencies and health care professionals.

THE "GRIEF" OF PRIVACY COMPLIANCE

By now, most Privacy Officers, Clinical Directors and Executive Directors at health care agencies across Ontario have journeyed through the "five stages of grief" of privacy compliance: *denying* that their practices have to change; *anger* at the upheaval this new legislation created in their day-to-day operations; *bargaining* with their clinical staff and management to implement the PHIPA-compliant policies they have developed; *depression* upon realizing that their information and privacy practices will be scrutinized whenever the agency seeks accreditation or if any slip is reported to Ontario's Privacy Commissioner; and finally, *acceptance* of the fact that the confidentiality, access, correction, and disclosure provisions under PHIPA are now and will forever be part of the everyday delivery of mental health services in this Province. This process has hopefully resulted in the implementation of policies and procedures that comply with PHIPA.

PRIVACY COMPLIANCE: THE ON-GOING CHALLENGE

Even with PHIPA-compliant policies and protocols, management of privacy issues presents a constant challenge on Privacy Officers and senior staff who work with PHIPA every day, as they struggle with tricky situations and new scenarios, such as:

- Under what circumstances can a child consent to the release of his or her PHI?
- Who can provide consent when custody for a child has been not been established?
- What if two parents give conflicting instructions?
- What if the child's decision conflicts with that of his or her parent(s)?
- When a concern arises about abuse, how much information can be shared with a Children's Aid Society?
- How are "lock box" requests addressed?
- How do you respond to a request to "correct" observations contained in a clinical worker's report?



- Under what circumstances can an agency deny a client access to his or her PHI record? How should the agency respond to such a request?
- How do you manage a privacy breach or complaint? What is to be disclosed? How, to whom, and when?
- Who is in each client's Circle of Care, and why does this matter?

Ensuring that staff have adequate training to manage these issues is the next step in privacy compliance, once an organization has the necessary policies and procedures in place.

WHAT DOES COMPLIANCE MEAN?

The managers and directors of those health care agencies that have completed the journey to privacy compliance take comfort in knowing that:

- They have a Privacy Officer who is aware of his or her role and obligations
- All agency staff know to forward to the Privacy Officer all requests for access or corrections to a personal health information record
- The agency's Statement of Information Practices is provided or made available to all clients
- Any questions about the agency's privacy practices can be answered by reviewing the agency's Privacy Policy, which complies with the legislation
- The agency only collects that personal health information (PHI) that is necessary for the delivery of services, and only collects, uses and discloses PHI with their clients' consent or where permitted or required by law
- Policies are in place to safeguard all PHI records and to prevent a privacy breach through the actions of staff members of agency volunteers (not only the "malicious", but also the "curious" and the "sloppy")
- When PHI is destroyed, it is done so in a secure and permanent matter

These documents and protocols form the basic components of privacy compliance, but it requires more than good practices and policies for a health care organization to develop a "culture of privacy".

WHAT IF WE AREN'T QUITE HIPAA-COMPLIANT YET?

Any agency that has not yet implemented policies to safeguard the PHI it collects, uses and discloses must make this an urgent priority. We can no longer hope or expect that Ontario's Information and Privacy Commissioner will excuse a preventable breach or well-founded complaint on the basis that the legislation is "still new". It is no longer enough for an agency to simply respect confidentiality and to take steps to safeguard their clients' records. The consequences of failing to



comply with PHIPA are significant: any health information custodian who fails to comply with PHIPA exposes him or herself to an Order from the Commissioner, a potential civil lawsuit, and a fine of up to \$50,000 (for an individual) and up to \$250,000 (for a corporation). In light of these potential consequences, if you have any questions as to whether your agency's privacy practices are adequate and PHIPA-compliant, the time to address these is now, before a breach or complaint triggers a review, investigation or even a published Order by the Commissioner.

OUR INFORMATION AND PRIVACY PRACTICES ARE PHIPA-COMPLIANT: NOW WHAT?

While PHIPA-compliant policies are a necessary first step, clients' PHI will only truly be protected when an agency has instilled a "culture of privacy", meaning that everyone who collects, uses and discloses PHI understands and complies with the agency's protocols and policies and their obligations under PHIPA. Without this, every agency is vulnerable, not only to a privacy breach or complaint, but to a public order by the Commissioner to do what the legislation requires of it, such as in the Privacy Commissioner's Second Order under PHIPA which involved a privacy breach at the Ottawa Hospital. The Commissioner observed that, **although the hospital had implemented various policies and procedures, it had not yet prioritized privacy or developed a "culture of privacy"**, and among other sanctions, the Commissioner ordered that all members of the hospital undergo training in the area of privacy.

HOW DO WE DEVELOP A "CULTURE OF PRIVACY"?

Once the agency has implemented the policy documents and protocols necessary for privacy compliance, the agency's management must ask themselves: ***Do all members of the agency have the knowledge base and tools necessary to prevent a privacy breach?***

Without a concerted effort to train front-line staff on PHIPA and each staff member's obligations respecting PHI, it is unlikely that the answer to this question is "yes". As privacy issues arise on a daily basis, a culture of privacy can only be developed within a health care agency through a commitment from the agency's management to giving all of an agency's staff members the resources and training they require to managing these issues. This requires training specific to the agency's information and privacy practices and with respect to PHIPA.