David Young Law
Compliance Bulletin

February 2018

New Ontario Breach Reporting Rules Respond to Snooping and Cybersecurity Concerns

On October 1, 2017, new rules requiring health information custodians (HICs) in Ontario to report breaches of personal health information to the Information and Privacy Commissioner (IPC) came into force. While the rules address specifically reporting in the health sector, the full breach response framework contains guidance relevant to all public sector entities and is instructive for the private sector.

Importantly, the rules contain a requirement for HICs to commence tracking all privacy breaches, whether reportable or not, effective January 1, 2018.

Response to the snooping issue

The new rules were adopted under Bill 119, the *Health Information Protection Act, 2016*. The bill included significant breach response and offence provisions, designed to address the increasingly urgent issue of snooping into personal health records. At the time of its passage, several significant and large health records breaches had occurred, perpetrated in every case by internal staff at healthcare institutions[1]. Ontario's health privacy legislation, the *Personal Health Information Protection Act, 2004* ("PHIPA"), contained only limited provisions enabling the IPC to address such breaches effectively. In particular, there was no requirement for such breaches to be reported to the IPC, and the ability of the IPC to prosecute perpetrators with a view to deterring future breaches was hampered by procedural limitations and inadequate financial penalties.[2] The new breach reporting protocol was one of the measures adopted to assist the IPC in addressing such breaches. The rules came into effect on October 1 of last year with the issuance of regulations provided for under the bill and stipulating the circumstances in which reports are required to be made.

Response to cybersecurity incidents

While the new breach reporting rules were designed to address the snooping-related health sector breaches, they also address and represent a timely response to the growing concern regarding cybersecurity and breach incidents globally. In this regard, their coming into force anticipates by only a matter of months the new mandatory breach reporting provisions under PIPEDA, Canada's national

[1] See for example: *Rouge Valley Health System*, PHIPA Order HO-013, Dec. 16, 2014; *Hopkins v. Kay* 2015 ONCA 112.

[2] Under Bill 119 the six-month limitation period for commencing a prosecution was eliminated and potential fines were increased to $100,000 for individuals and $500,000 for corporations (from $50,000 and $250,000).

private sector privacy law. The new PIPEDA rules require not only breach reporting but also notification of affected individuals – required under PHIPA even before the passage of the new breach reporting rules,[3] as well as a requirement to keep records of all breaches, whether not reported.[4] It is significant to note that in addition to the obligations to report under the new PHIPA rules, a HIC will be required to report to the IPC the number of breaches it has experienced in each year – a stipulation that implies a record-keeping requirement as under the PIPEDA rules.

It is clear under both new breach reporting regimes - Ontario and federal - that the regulators are not only looking to obtain information that may indicate a failure to comply with legislation but are also seeking to build knowledge bases that will enable them to understand the causes of breaches and to take measures to encourage data custodians to improve their security systems and protect the personal information of their constituents whether they be recipients of health care or members of the public generally.

What breaches must be reported

The new PHIPA requirements provide that reports must be made to the IPC in defined circumstances, as set out in the *PHIPA Regulations*. The circumstances in which breach reports must be made are as follows:

1. PHI in the custody of the HIC has been used or disclosed without authority by a person who knew or ought to have known that they were doing so.
2. PHI in the custody or control of a HIC was stolen.
3. PHI subject of an initial breach, whether or not reported, has been or may be further used or disclosed without authority.
4. The loss or unauthorized use or disclosure of PHI is part of a pattern of similar losses or unauthorized uses or disclosures of PHI in the custody or control of the HIC.
5. The HIC is required to give notice to a college of health professionals pursuant to section 17.1 of PHIPA regarding a loss or unauthorized use or disclosure of PHI.
6. The HIC would be required to give notice to a college in circumstances described in section 17.1 involving an employee of the HIC who is not a member of a college.
7. The loss or unauthorized use or disclosure of PHI is significant in the circumstances including whether the PHI is sensitive, the breach involved a large volume of PHI or a large number of individuals, and whether more than one HIC or agent of a HIC was involved in the breach.

Usefully, the Ontario Information and Privacy Commissioner has issued guidance to assist in determining when such reports should be made and what they should include.

[3] PHIPA section 12(2).
[4] PIPEDA section 10.3(1); see also *Compliance Bulletin*, September 2017, "Proposed Breach of Security Safeguards Regulations published".

In its guideline, *Reporting a Privacy Breach to the Commissioner*, the IPC makes clear that an accidental or inadvertent breach that otherwise would fall within the first category, does not require a report to the IPC if it is a single isolated incident. Such circumstance could include a misdirected fax or mail delivery, or an inadvertent or accidental accessing of a personal health record. However if such an initial breach is compounded by, or becomes part of, any of the other specifically listed circumstances – for example, a pattern of similar incidents or involves sensitive PHI, then reporting would be required, under categories 4 or 7.

Information to be included in a report to the IPC

The IPC has published a Privacy Breach Report Form setting out the information that it expects to be included in a report, including a description of the circumstances of the breach including its cause, the PHI involved, when and how it was discovered, whether any agents of the HIC or any other HICs were involved, and the number of individuals whose PHI was affected. In addition, the report must describe the steps taken to contain and respond to the breach, whether the affected individuals were notified and if so particulars of such notification. Finally, the report must describe steps taken by the HIC for investigation, remediation and prevention of future breaches.

The breach report form follows closely the IPC's guidance to HICs and public sector institutions for a breach response protocol. It is clear that the IPC, under its new breach reporting authority, will be looking to use the information provided in reports to assess the adequacy of steps taken to respond to a breach and, as needed, to recommend any adjustments or further steps, as well as to provide it with information should it decide to pursue remedial action against the HIC or the perpetrators of the breach.

Requirement to notify Health Professions College

Bill 119 was part of a multi-pronged strategy to combat health sector snooping and other breaches. It also included provisions requiring HICs to notify a professional college where a member of that college is employed by the HIC or the HIC has extended privileges to or is otherwise affiliated with a member of the college, where it has been determined that the member was involved in a breach and disciplinary action has been taken, or the member has resigned from the HIC or the member's privileges or affiliation have been terminated or restricted, in either case as a result of an investigation related to the breach.

The rationale for requiring notification to a professional college is to have the college also take disciplinary action against the member, if justified, as a result of their involvement in a breach, including potentially suspending or terminating the right to practice their profession. The objectives are two-fold. Firstly, the aim is to prevent future breaches through, potentially, removing the perpetrator from the ability to cause such breaches by denying them such opportunity through practicing their profession.

Secondly, the broader goal is to support the prevention objective through deterrence by making clear that serious professional sanctions may be imposed on anyone involved in such a breach in the future.

The requirement to notify health professions colleges parallels two categories of circumstances requiring reporting a breach to the IPC: where the person implicated is a member of a college, and where, even if not a member, they are an employee or other agent of the HIC if the circumstances would have required notification had they been a member.

Requirement to file annual report regarding breaches

The breach reporting regulation also includes a significant requirement for every HIC to file with the IPC, annually, a report of the number of incidents involving the theft, loss or unauthorized use or disclosure of PHI under its custody or control occurring in each year. This reporting requirement is effective commencing March 1, 2019, for the 2018 year.

The IPC has provided guidance regarding the detailed breakdown of statistics that it will require to be included in such reports, which breakdown must include in effect a description of the cause of each breach. The IPC's guidance makes it clear that this annual reporting requirement extends to breaches for which a HIC has not separately provided a report to the IPC. As a result, HICs will need to create and maintain records of *all* breaches, including those caused by accident or inadvertence.

As noted, the annual report provision, implying a requirement to maintain records of all breaches whether or not any are separately reportable, parallels the requirement under the new PIPEDA mandatory breach reporting rules, for organizations to maintain records of all breaches.[5] The legislative and regulatory objectives of prevention and protection are again evident in this annual reporting requirement. By requiring HICs to report and potentially have their ongoing privacy breach experience made public, they should have strong motivation to enhance their internal breach prevention procedures. Furthermore, the IPC, through its collection of this aggregate data, aims to increase its understanding of the causes of breaches with a view to providing guidance and, potentially, recommending additional legislative initiatives for future breach prevention.

For more information please contact:

David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.

[5] By contrast however, the PIPEDA requirement does not mandate organizations to file publicly any statistical or other report summarizing the organization's history of breaches.