BLG PUBLICATION

Borden Ladner Gervais

Reporting PHIPA Breaches to Affected Individuals and the Information and Privacy Commissioner: A Primer

Wednesday, December 5, 2018

Under Ontario's *Personal Health Information Protection Act* (PHIPA), hospitals and other health information custodians (HICs) are potentially subject to a number of requirements when confronted with a privacy breach. When PHIPA was first enacted, these requirements focused primarily on remediating the breach and notifying the affected patient. Now, however, HICs must report certain individual PHIPA breaches to the Information and Privacy Commissioner of Ontario (IPC). In addition, starting in 2019, they will also be required to provide annual reports on breaches. Of note, the circumstances in which these different reporting obligations are triggered can vary; the deadlines for making the reports are not uniform; and the required content for the reports differ. All of this can be confusing. This article provides a brief summary of these different reporting obligations to help HICs better understand their obligations under PHIPA.

Reporting a breach to an affected individual

The obligation to notify an affected individual about a breach has been in force for some time. It requires an HIC to notify an individual if personal health information about the individual "is stolen or lost or if it is used or disclosed without authority". By "used," PHIPA appears to mean "viewed" or "handled" as well. The specific requirements surrounding this reporting obligation are as follows:

- **When:** PHIPA does not impose a specific deadline for notification, though it does require that the notification be carried out "at the first reasonable opportunity". Guidance materials issued by the IPC urge that an HIC that has contacted law enforcement authorities should first speak with those authorities about whether to delay notification in order not to impede a criminal investigation.
- **How**: PHIPA does not mandate a certain form of notification, though IPC guidance materials urge that the notification generally be direct (by phone, letter, or in person) and that indirect notification (by website, posted notices, etc.) would be appropriate only in certain circumstances.
- **What to include**: PHIPA itself says little about the required content for such a notification, except that it should inform the affected individuals of their right to make a complaint with the IPC. However, the guidance materials instruct HICs to also include:
    - the date of the breach;
    - a description of the nature and scope of the breach;
    - the name of the agent responsible for the unauthorized access where appropriate;
    - a description of the information involved;

- steps taken to control or reduce the harm;
- steps planned to be taken to prevent further breaches;
- steps the individual can take to enhance personal protection; and,
- contact information for someone in the organization who can answer additional questions.

The guidance documents also offer sample language that can be added to a notification letter in a matter involving financial information or health card numbers.

Reporting a breach to the IPC: annual reports and ongoing breach-specific reports

In addition, PHIPA now establishes two separate sets of requirements to report breaches to the IPC, the newer of which is the annual reporting requirement, which will come into effect in 2019. The same types of incidents about which the HIC must notify affected individuals are the ones that the HIC must include in its annual report — that is, incidents in which personal health information was stolen, lost, or used or disclosed without authority. The specific requirements for the annual report are as follows:

- **When**: The report is due on or before March 1 of each year, commencing on March 1, 2019. Each report will set forth the required information in respect of the previous calendar year (in other words, the report that each HIC will file between January 1 and March 1, 2019 will address breaches that took place during calendar year 2018).
- **How**: The report will be submitted electronically, though the e-form is not presently available.
- **What to include**: The IPC has issued a guidance document that indicates that the following information will be required in each annual report:
    - For cases involving stolen information: the total number of such cases; the number of cases involving theft by an internal party, theft by a stranger, theft via ransomware attack, theft via other cyberattack, theft of an unencrypted portable device, theft of paper records; the numbers of individuals affected.
    - For cases involving lost information: the total number of such cases; the number of cases involving loss due to ransomware attack, loss due to other cyberattack, loss of an unencrypted portable device, loss of paper records; the numbers of individuals affected.
    - For cases involving information used (*e.g.*, viewed, handled) without authority: the total number of such cases; the number of cases involving unauthorized use through electronic systems and unauthorized use through paper records; the numbers of individuals affected.
    - For cases involving information disclosed without authority: the total number of such cases; the number of cases involving unauthorized disclosure through misdirected faxes and unauthorized disclosure through misdirected e-mails; the numbers of individuals affected.

Additionally, a separate IPC reporting obligation applies to individual breaches that meet a particular severity threshold. HICs must report these breaches to the IPC on an ongoing basis throughout the year, and in more detail than is needed for the purpose of the annual report. Because only certain breaches will be subject to this requirement, the number of breaches reported individually to the IPC under this provision will be smaller than the total number of breaches reported in the annual IPC breach report discussed above.

Breaches must be reported to the IPC individually if the following conditions are met:

- The HIC has reasonable grounds to believe that the information was used or disclosed without authority by a person who knew or ought to have known that he or she was acting without authority (for example, an accidentally mis-delivered fax would not meet this requirement, but a case of deliberate "chart snooping" would);
- The HIC has reasonable grounds to believe that the information was stolen;
- The HIC has reasonable grounds to believe that the information, after being initially lost or used or disclosed without authority, was or will be further used or disclosed without authority;
- The HIC is required to give notice of the incident to a College under the *Regulated Health Professions Act* (the requirements for notice to the College are articulated elsewhere in PHIPA and are not summarized here); or
- The HIC determines that the incident is "significant" after considering "all relevant circumstances" including the sensitivity of the information, the volume of the information, the number of affected individuals, and whether more than one HIC or HIC agent was responsible for the incident.

The specific requirements for the individual breach report to the IPC are as follows:

- **When**: Though PHIPA is silent as to the timing of the report, it would be prudent to notify the IPC reasonably soon after concluding that a report is required, based on the circumstances outlined above. The online breach report form expressly acknowledges that at the time the breach is reported, the investigation, containment, and remediation of the breach may not be completed, and asks that the HIC provide as much of the requested information as is presently known.
- **How:** The individual breach report is to be completed and submitted electronically.
- **What to include:** The online form requests information about the breach incident itself (what happened, how it was discovered, the dates of the breach and its discovery, the nature of the information, the number of affected individuals, how many agents of the HIC and how many other HICs were involved in the breach); containment (steps taken by or at the direction of the HIC to contain the breach, the date of such steps and their outcome); breach notification (date, method, content of notification); and investigation and remediation/prevention steps.

AUTHOR

Ira Parghi
T 416.367.6458
IParghi@blg.com

Borden Ladner Gervais

BLG OFFICES

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T +1.403.232.9500
F +1.403.266.1395

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T +1.514.954.2555
F +1.514.879.9015

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T +1.613.237.5160
F +1.613.230.8842

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415