BLG PUBLICATION

Borden Ladner Gervais

Mandatory Reporting of Privacy Breaches to the Information and Privacy Commissioner now required under the Personal Health Information Protection Act, 2004

Tuesday, July 11, 2017

In June 2016, the *Personal Health Information Protection Act, 2004* ("PHIPA") was amended to require that custodians provide notice to the Information and Privacy Commissioner of Ontario if the circumstances surrounding a theft, loss or unauthorized use or disclosure met certain requirements. In June of this year, the regulations setting out those circumstances were published and are found at section 6.3 of O. Reg 329/04. They are slated to come into force on October 1, 2017.

The following will outline the sometimes overlapping circumstances in which notification to the Commissioner is required. Overall, notification to the Commissioner will be required in almost all cases in which a patient has received a notice under section 12 of PHIPA.

Where Information Has Been Lost, Stolen or Used or Disclosed Without Authority

Under subsection 6.3(1)(1.) of the regulations, a health information custodian ("Custodians") will be required to notify the Commissioner where it has reasonable grounds to believe that personal health information in its custody or control "was used or disclosed without authority by a person who knew or ought to have known" that he or she did not have permission to do so. In particular, notification will be required in cases of snooping or reckless handling of personal health information. On the other hand, a custodian may not be required to notify the Commissioner where information was inadvertently viewed or disclosed.

Custodians are also required to notify the Commissioner where they have reasonable grounds to believe that personal health information has been stolen under subsection 6.3(1)(2.). Or, where there was or will be further disclosure of PHI that was lost, used or disclosed without authority under subsection 6.3(1)(3.). These circumstances ensure that the Commissioner is made aware of situations in which the privacy breach is not self-contained or whether there is a risk of a continuing privacy breach.

The Commissioner will also need to be notified where there has been a pattern of similar losses of personal health information or of unauthorized use or disclosure. For example, notification would be required if a custodian experienced a series of inadvertent disclosures or losses due to a fax machine error or other systemic issue.

Additional Circumstances

The regulation also includes two additional circumstances in which notification is required: 1) where an agent has been disciplined, and 2) where the privacy breach is "significant".

1. Discipline of agents for privacy breaches

The amendments to PHIPA made in June of 2016 introduced section 17.1 which required custodians to report agents to their regulatory college if they were disciplined for the

"unauthorized collection, use, disclosure, retention or disposal of personal health information" or resigned in anticipation of discipline.

Subsection 6.3(1)(5.) of the regulations piggy-backs on those changes and requires that the Commissioner receive notice where notice to a College has been given. The regulations, under subsection 6.3(1)(6.), extend the requirement to notify the Commissioner in respect of agents who are not members of a regulatory College in the same circumstances. In practice, these sections will require that Custodians notify the Commissioner anytime an agent is disciplined for a privacy breach.

2. "Significant" privacy breaches

The last circumstance in which the Commissioner must be notified is where the loss or unauthorized use or disclosure is "significant". The term, "significant", is not defined in the regulations of the Act. Subsection 6.3(1)(7.), however, lists four factors that a Custodian should consider in order to determine whether notification is required:

1. Whether the personal health information at issue is sensitive;
2. Whether the breach involved a large volume of information;
3. The number of individuals the information relates to; and
4. The number of health information custodians involved.

The goal of this subsection is to capture any large or extensive privacy breach which was not captured by the previous circumstances.

Conclusion

The purpose of these regulations is to require notification to the Commissioner in nearly all situations where there is a privacy breach which required patient notification. At least initially, this will likely generate a significant increase in the number of notifications to the Commissioner. This may also result in a corresponding increase in investigations and orders. As the regulations do not go into effect until October 1, 2017, this is a good opportunity for Custodians to review policies and procedures and to communicate to all agents that privacy breaches they are involved in may need to be reported to the Commissioner.

AUTHOR

Roberto Ghignone
T 613.369.4791
RGhignone@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