No need for access, theft or disclosure: encryption of data is notifiable under PHIPA and CYFSA

September 25, 2025

In *Hospital for Sick Children v. Ontario (Information and Privacy Commissioner)*, 2025 ONSC 5208, the Divisional Court clarified that the notification obligations in the *Personal Health Information Protection Act, 2004* (PHIPA) and the *Child, Youth and Family Services Act, 2017* (CYFSA) apply when a ransomware attack makes personal health information or personal information inaccessible, even if only temporarily, and there is no evidence the information was actually viewed, accessed or stolen.

Background

In 2022, the Hospital for Sick Children (SickKids) and Halton Children's Aid Society (Halton) experienced separate ransomware attacks.

These attacks encrypted the SickKids and Halton servers where files containing personal information were stored, preventing access to these files. However, there was no evidence the threat actor viewed, accessed, or stole any files containing personal information. Both SickKids and Halton had robust backup policies in place that allowed the files to be quickly restored. The attacks resulted in minor service delays in diagnostic and treatment for a small number of patients at SickKids, and had little impact on Halton's internal systems and did not disrupt services. SickKids posted notices on its website about the cyberattack and the resulting delays in diagnostics and treatment services. Halton did not notify the public about the cyberattack because there was no impact on clients' information, or the services available to them to report.

The IPC decisions

In two separate decisions, the IPC found that although the threat actors did not view, access or take any individual files housed within the encrypted environments, the attacks constituted an unauthorised "use" and "loss" of personal information under PHIPA and CYFSA, and therefore triggered the notification requirement to individuals whose data was impacted. The IPC concluded that the encryption of the servers was an unauthorised "use" because at a minimum, the ransomware made the information

unavailable and inaccessible to authorised users of that information, and concluded the attack amounted to a loss because, for at least some period of time, the information became unavailable to authorised users because of an unauthorised activity.

In the SickKids decision, the IPC noted the hospital made appropriate public disclosure in the aftermath of the attack, but this notice did not comply with the notification requirement at s. 12(2) of PHIPA because it did not include information about the right to complain to the IPC. Given the passage of time, the IPC said there was no utility in ordering SickKids to provide notice of the right to complain at the time it issued its decision, and made no further remedial orders.

In the Halton decision, the IPC found that Halton did not comply with the notification requirement at s. 308(2) of the CYFA because it did not notify individuals directly and issued no other public notice of the incident. However, applying a contextual and flexible approach to notification, the IPC was satisfied Halton could meet the notification requirement by posting a general notice on its website or issuing a public release.

The Divisional Court's decision

On appeal, the Divisional Court upheld the IPC's interpretation of "use" and "loss" and the finding that SickKids and Halton (the Applicants) were required to notify individuals about the ransomware attacks. The Ontario Hospital Association (OHA) intervened to provide the Court with the statutory context behind risk-based thresholds in other pieces of Canadian privacy legislation, cautioning that a notification requirement for ransomware attacks where data is not directly accessed or stolen risks unnecessary over-notification and can lead to needless costs, unnecessarily raise anxiety levels and lead to notification fatigue among individuals.

The Court upheld the IPC's "purposive" approach to interpreting the notification requirements under PHIPA and CYFSA, which found that the ransomware attacks' effect of making information temporarily unavailable was a kind of *handling* or *dealing with* that information in accordance with the word "use" in PHIPA and CYFSA, and that as a result of the unauthorised "use", the duty to notify under both statutes was triggered. The Court found this interpretation was justified based on the text, context, and purpose of the notification requirements in each statute.

The Court concluded the text of the statute suggested that unauthorised "uses" can occur without direct interaction with information, as it did in this case, and as it might if a physical hard drive with information is destroyed, thereby disposing of that information.

With respect to the context and purpose, the Court noted that s. 12(2) of PHIPA and s. 308(2) of CYFSA are not tied to a risk of harm (unlike other Canadian privacy statutes, which contain risk-based notification thresholds such as real risk of significant harm). Rather, the notification requirements recognise "individuals' continuing interest in their personal information and in ensuring that information custodians are transparent and accountable."

The Court concluded the purpose of notification is not only to advise affected individuals of risks in order to mitigate harm but includes ensuring custodians are accountable for how they protect individuals' personal information and enabling the IPC to exercise its

authority to provide oversight of Ontario's privacy regime and ensure proper investigations are conducted.

Key takeaways for custodians subject to PHIPA or CYFSA

- The purpose of notification in PHIPA and CYFSA is about ensuring transparency and accountability. Notification recognises that individuals have a continuing interest in their personal information and ensuring that information custodians are transparent and accountable. Notification also enables the IPC to exercise its authority to provide oversight of Ontario's privacy regime and ensure proper investigations are conducted in the aftermath of cyber attacks.
- Following a ransomware attack, notification is required under PHIPA and CYFSA even in cases where information is not actually viewed, accessed, or misused, and it was only temporarily inaccessible.
- The IPC applies a contextual and flexible approach to determining the appropriate form of notice in certain the circumstances. In considering whether indirection notification may be appropriate, the relevant factors include: the number of potentially affected individuals, the nature and volume of the information at issue, the difficulty of determining with certainty exactly which individuals, and what information, had been affected by the attack, the remedial actions of the custodian, and the passage of time.
- The new notification obligation in *Freedom of Information and Protection of Privacy Act* (FIPPA) came into effect on July 1, 2025. Notification under FIPPA is required where there is a real risk of significant harm. Custodians like hospitals, subject to both PHIPA and FIPPA, will need to be mindful of the different notification obligations that may apply from one security or privacy incident.

By

Eric S. Charleston, Daniel Girlando, Hanna Rioseco

Expertise

Cybersecurity, Privacy & Data Protection, Health Law

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

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

T 403.232.9500
F 403.266.1395

Ottawa

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

T 613.237.5160
F 613.230.8842

Vancouver

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

T 604.687.5744
F 604.687.1415

Montréal

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

T 514.954.2555
F 514.879.9015

Toronto

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

T 416.367.6000
F 416.367.6749