SIGNIFICANT EXPANSION OF ONTARIO'S PERSONAL HEALTH INFORMATION PROTECTIONS AMID COVID-19: WHAT YOU NEED TO KNOW

Posted on July 15, 2020

Categories: Insights, Publications

Amid the COVID-19 pandemic, accessing healthcare and personal health information ("**PHI**") online has become increasingly prevalent. Ontario's *Personal Health Information Protection Act* ("**PHIPA**") provides rules that govern the collection, use and disclosure of PHI to protect privacy and confidentiality. On March 25, 2020, Bill 188 received royal assent, making significant amendments to PHIPA, many of which affect technology companies (and potentially some insurers) who process and provide access to PHI.[1] These include the creation of a new category of entity subject to PHIPA ("consumer electronic service providers"), the introduction of mandatory electronic audit logs, and new de-identification standards. The changes discussed here, other than those which effect penalties under PHIPA, will come into force on a date to be named by the Lieutenant Governor.

Consumer Electronic Service Providers

One of the most notable changes under Bill 188 creates a new category of entity subject to PHIPA – "**consumer electronic service providers**". By definition, these entities provide electronic services to individuals for the purpose of, among other things, allowing individuals to access, modify or otherwise manage their PHI records. This directly targets consumer-facing technology developers and service providers, who were previously subject to few, if any, obligations under PHIPA. In addition, the broad language within the amendments may increase the scope to include any person or entity involved in a platform that allows for the access, modification or other management of PHI records – potentially including insurers who allow insureds to store, manage and/or process PHI electronically, such as through an app or portal for online claim submissions. Under these amendments, all such companies will be directly subject to PHIPA and the increased protections and penalties under these amendments.

The amendments also set in law the right of individuals to use electronic means to access their records through these consumer electronic service providers. This provides individuals with more control over their PHI. They also provide for oversight of these services by the Privacy Commissioner of Ontario (the

"**Commissioner**"). This oversight includes the ability for the Commissioner to conduct a review of a particular service provider and prevent health custodians from sharing PHI with particular services if there are concerns regarding their privacy policies. The Commissioner released a statement that stresses the importance of how these amendments protect the right of individuals to manage their PHI and provide oversight and protection against unauthorized attempts to access patient PHI.[2]

Subsequent regulations will set out specific requirements and exceptions for consumer electronic service providers. Technology companies and insurers should be mindful of the requirements, restrictions and penalties that these amendments bring, and how subsequent regulations may impose additional obligations.

Electronic Audit Logs

Health Information Custodians ("**HICs**"), including health care practitioners, hospitals, pharmacies, long-term care homes and other individuals or institutions that have custody or control of PHI, are now required to maintain, monitor and audit "**electronic audit logs**". This requirement includes all PHI that is accessible via electronic means, thus extends to any customer electronic service providers to which HICs provide PHI.

These electronic audit logs must track all activity relating to a record or part of a record of PHI that is accessible by electronic means. For every instance that a record or part of a record is viewed, handled, modified or otherwise dealt with, the log must state:

1. The type of information accessed
2. The date and time of the activity
3. The identity of the person(s) who accessed the PHI
4. The identity of the person to whom the PHI relates
5. Any other information required by subsequent regulations

These logs must be regularly audited and monitored by the HICs. Therefore HICs will require adequate functionality from their electronic service providers in order to satisfy these requirements. Additionally, the Commissioner may request electronic audit logs at any time to verify compliance with PHIPA. By increasing oversight and mandating the creation, monitoring, and auditing of these logs, patient privacy is significantly strengthened.

Increased Enforcement and Penalties

The amendments expand the powers of the Commissioner to enforce PHIPA, including allowing the Commissioner to order the production of evidence regarding a suspected offence. The amendments also make it clear that these administrative penalties do not prohibit individuals from seeking another form of remedy, such as a breach of privacy tort at common law.

This new enforcement regime could result in significant fines for those who handle PHI, including consumer electronic service providers, if they fail to properly handle and protect PHI. This extends to any officers, employees or agents of corporations if they authorize or knowingly refrain from using their authority to prevent an offence from being committed, even if the corporation itself is not prosecuted or convicted.

Indeed, the maximum fines under PHIPA have doubled and are now $200,000 for individuals and $1,000,000 for corporations. There is also a potential for up to one year of imprisonment for individuals. While there is a two-year limitation period to impose administrative penalties from the time of the offending action or inaction, this may be disregarded for a series of contraventions if the most recent contravention is within the limitation period.

Perhaps most significantly, fines can now be given directly by the Commissioner, which may be issued for the purposes of encouraging PHIPA compliance or preventing an individual from deriving any economic benefit resulting from a contravention of PHIPA (including through negligent acts). Previously, fines were limited to deliberate actions which constituted an offence and did not extend to negligence.

In light of this increased liability, HICs and consumer electronic service providers will need to re-evaluate their policies and practices to ensure compliance with the existing and amended rules and regulations under PHIPA. In addition, companies that handle any PHI – such as insurance providers who provide services through web-based platforms – should carefully consider whether they are subject to these amendments.

Amendments to the Freedom of Information and Protection of Privacy Act ("FIPPA")

In addition to the amendments to PHIPA, Bill 188 introduced the definition of an "extra-ministerial data integration unit" under FIPPA. This definition allows defined non-public sector entities to collect PHI as well as data from the province for the purpose of compiling statistical information which will aid in managing and allocating resources, planning, and evaluating programs and services. These entities will also be regulated under PHIPA and thus subject to the enhanced protections provided by the amendments.

The Future of Privacy Regulations

The recent and pending changes to the legislation echo the concerns voiced by the privacy commissioners and the public regarding the privacy protections built into the national contact-tracing app that will be launched in the coming weeks.[3] With more of Canadians' sensitive information being accessed through third-party applications, privacy considerations will become increasingly important. In addition to the changes discussed here, the amendments refer to a new definition of "de-identify" that will be set out in regulations at a later date. This will include specific de-identification requirements and will likely set a minimum legal standard for all entities subject to PHIPA. This suggests that further regulations will continue to increase the burden on

those who handle PHI to improve patient privacy and the security of sensitive health records.

The federal and provincial privacy commissioners continue to urge legislators to modernize Canadian privacy legislation. Currently, the commissioners are conducting an investigation into the regulation of biometrics, including noteworthy technology such as Clearwater AI.[4]

The amendments set out in Bill 188 pave the way for other provinces to enact similar legislation that expands privacy protections where third-party providers access and gather sensitive, personal information. Any entity who might possibly fall within the definition of a consumer electronic service provider should keep a careful eye on these developments.

by Darcy Ammerman, Grace Shaw and Kristen Shaw (Summer Law Student)

[1] Bill 188, An Act to enact and amend various statutes, 1st Sess, 42nd Leg, Ontario, 2020 (assented to 25 March 2020), SO 2020, c 5.
[2] Brian Therrien, "How government's response to COVID-19 ushered in new privacy protections" (31 March 2020), online: Information and Privacy Commissioner of Ontario.
[3] Catharine Tunney, "Voluntary nationwide contact tracing app coming soon, says Trudeau" (18 June 2020).
[4] Office of the Privacy Commissioner of Canada, Announcement "Commissioners launch joint investigation into Clearview AI amid growing concerns over use of facial recognition technology" (21 February 2020).

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.