PHIPA Amendments: What They Mean for Your Practice of Handling Personal Health Information

June 1, 2020

Over the last year, the Ontario government has passed two bills that introduce notable amendments to the *Personal Health Information Protection Act, 2004* ("PHIPA"). These changes are especially important for organizations that electronically collect, process and store personal health information ("PHI"), such as technology companies doing business within the digital health sector.

First, Bill 138, the *Plan to Build Ontario Together Act, 2019* ("Bill 138") establishes limitations on the use of de-identified information and introduces new regulation making powers.

Second, Bill 188, the *Economic and Fiscal Update Act, 2020* ("Bill 188") provides for, among other things, mandatory electronic audit logs and regulation of "consumer electronic service providers".

By way of background, PHIPA is the provincial legislation that governs the collection, use and disclosure of PHI within the health sector to protect an individual's privacy and confidentiality of information. PHI is defined as identifying information about an individual relating to their physical or mental health. PHIPA applies to (i) health information custodians (i.e. persons and organizations with custody or control over PHI, such as primary care providers, hospitals, pharmacies and certain community care organizations); (ii) agents authorized to act on behalf of such custodians (e.g. hospital employees and third-party service providers); and (iii) those receiving PHI from custodians.

This commentary highlights some of the significant amendments enacted through Bill 138 and Bill 188 that are not yet in force and why organizations dealing with electronically-stored PHI should be prepared for these changes once they become enforceable. Note that this information presented here is subject to change, as further amendments may be adopted in the future.

1. Bill 138, the *Plan to Build Ontario Together Act, 2019*

Bill 138 is an omnibus bill that received Royal Assent on December 10, 2019 and amends a large number of provincial statutes. Schedule 30 of Bill 138 presents a number of PHIPA amendments that are not yet in effect. The major changes are detailed below.

a) Limiting Use of De-identified Information

New section 11.2 of PHIPA prohibits any person, except for health information custodians and other prescribed persons, from using or attempting to use de-identified information to identify an individual, either alone or in combination with other information. To enforce this provision, a new statutory offence under section 72(1) has been added whereby a person or an organization that "willfully contravenes" section 11.2 may be subject to a substantial administrative fine under PHIPA.

This amendment is broad enough to apply to most businesses, including those not directly governed by PHIPA. As such, businesses handling de-identified information must review their

practices to ensure they are compliant with the restriction once it comes into effect. For clarity, businesses should consider specifying in their privacy policies that any de-identified PHI in their control will not be used, either alone or with other information, to identify a specific individual to whom the information belongs.

b) New Regulation Making Powers

New regulation making powers are established under section 73(1) of PHIPA to enable, among other things, the circumstances under which Ontario Health or other entity designated as an integrated care delivery system may collect, use and disclose PHI, to be prescribed. Furthermore, regulations may be developed with respect to a health information custodian's use of electronic means to collect, use, modify, disclose, retain or dispose of PHI, including prescribing the process for setting, monitoring and enforcing such requirements.

Accordingly, it is expected that new regulations governing electronic PHI records will be introduced sometime in the future that would impact how custodians and their service providers operate and manage electronic PHI records. Therefore, technology companies assisting custodians with managing their electronic information systems should monitor any regulations that may be issued in the future to determine whether, as a result of such regulations, changes will be required in their contractual relationships to remain in compliance with PHIPA.

2. Bill 188, the *Economic and Fiscal Update Act, 2020*

Bill 188 received Royal Assent on March 25, 2020 and its Schedule 6 proposes several amendments to PHIPA. Some of these changes are now in effect, but the major amendments have not yet been proclaimed in force and are summarized below.

a) Mandatory Electronic Audit Log

Health information custodians who use electronic means to manage PHI will be required to maintain, audit and monitor an electronic audit log. The new obligation in section 10.1 of PHIPA specifies that the audit log *must* include the following information, for *every* instance a record (or part of a record) containing PHI is viewed, handled, modified or *otherwise dealt with*:

- the type of information that was accessed;
- the date and time it was accessed;
- the identity of all persons who accessed the PHI; and
- the identity of the individual to whom the accessed PHI relates.

Additional requirements about the electronic log, such as how long it must be retained, may be further prescribed by regulation.

Custodians are also required to provide, upon request, a copy of the electronic log to Ontario's Information and Privacy Commissioner (the "IPC"), even if it contains PHI. This is meant to promote accountability and oversee the custodian's compliance with PHIPA, while discouraging and checking for unauthorized access to digital PHI records.

While the obligation to maintain an electronic audit log is not yet in effect, custodians and their electronic service providers should now take the time to verify the technological capabilities of their electronic record systems and examine solutions to generate such audit logs in order to comply with any requirements that may be prescribed.

b) Consumer Electronic Service Providers

A new class of entities is established under section 54.1 of PHIPA – the consumer electronic service providers (the "CESPs"). A CESP is defined as a "person who provides electronic services to individuals at their request, primarily for the purpose of allowing those individuals to access, use, disclose, modify, maintain or otherwise manage their records of personal health information". As such, businesses that provide services *directly* to individuals involving their electronic PHI records will be subject to PHIPA.

Once the amendments take effect, CESPs will have to comply with prescribed requirements when providing electronic services to individuals. Furthermore, custodians that provide PHI to CESPs will have to comply with prescribed requirements and procedures. Therefore, CESPs will be governed as to how they collect, use and disclose PHI, and the use of their services by individuals and custodians. To date, details of such requirements are unknown and will be enacted in future regulations.

Businesses that provide electronic services to individuals involving their PHI should keep informed about the legislative developments impacting their information management practices. Once regulations governing CESPs are made available, these businesses should re-visit their operations to better prepare themselves for the new regime.

c) De-identification Standards

The definition of "de-identify" under PHIPA is amended to mean "to remove, *in accordance with such requirements as may be prescribed*, any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual". Therefore, new de-identification standards may be further set out in regulations and may potentially codify existing IPC guidance around de-identification to reduce the risk of re-identification.

3. Takeaways and a Note on Enforcement

The PHIPA amendments introduced in Bill 138 and Bill 188 represent one of the ways by which the Ontario government is looking to bring the health care sector into the 21st century, create an integrated health system and adopt new digital practices. However, an increased reliance on digital records poses additional information security and privacy risks to individuals. The new amendments are aimed at alleviating some of these risks, for example, by restricting re-identification, keeping electronic audit logs and regulating the use of PHI by CESPs.

Even though these amendments are not yet in effect, health information custodians, their technology service providers and others dealing with electronic PHI records should keep an eye on these changes to ensure their readiness to comply with the amendments once in force. This is largely because of the tougher enforcement measures recently enacted for violations of PHIPA.

First, the IPC has a new power to order an administrative penalty under section 61.1 to those who have contravened PHIPA or its regulations. Second, the penalties for offences under PHIPA have doubled as per subsection 72(2). The possible maximum penalty is $200,000 with potentially one year of imprisonment for an individual found liable for an offence under PHIPA and a penalty of $1,000,000 if the offender is an organization. Finally, these enforcement measures are not exclusive remedies as contemplated in section 65.1 of PHIPA, meaning that an administrative penalty could be combined with another enforcement measures or remedies available in law with respect to the same PHIPA violation, such as liability for privacy breaches under common law.

Because the consequences for non-compliance can be significant, organizations affected by these PHIPA amendments are advised to remain on top of new legislative developments and be ready to implement the necessary information management practices in the future.

If you have further questions, please contact a member of our technology law group.