HEALTH PRIVACY REVISITED – UPCOMING CHANGES TO ONTARIO'S HEALTH PRIVACY LAWS

Posted on August 11, 2015

Categories: Insights, Publications

Privacy matters to Ontarians and even more so, in light of a number of highly publicized breaches of sensitive personal health information ("**PHI**") in circumstances where one would expect PHI to be protected and treated with the utmost confidentiality. As well, there has been increasing pressure to modernize the province's health privacy laws as a result of changing health care delivery models, electronic health records and the collaboration among a greater number of individuals involved in the provision of a patient's health care. With this mind, Ontario's Health Minister Eric Hoskins has announced the government's commitment to privacy and accountability in the health care system and to amend the *Personal Health Information Protection Act* ("**PHIPA**"). While PHIPA is a relatively new piece of legislation in Ontario, having being introduced just over ten years ago, many stakeholders believe that it needs to be updated to reflect growing privacy concerns as well as to better align itself with recent changes made to the federal privacy legislation that governs commercial activities in the private sector - the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"). PHIPA has been deemed to be substantially similar to PIPEDA and as such, recent amendments to PIPEDA that include provisions that now make it easier to prosecute offences as well as those that impose increased fines for non-compliance, must also make their way into PHIPA.

On May 29, 2013, the Ontario government introduced Bill 78, the *Electronic Personal Health Information Protection Act* ("**EPHIPA**") to amend PHIPA with a focus on information sharing and coordination among health care providers involved in a patient's circle of care, through the creation of a single, provincial electronic health record maintained by "prescribed organizations." While no specific prescribed organization was listed in Bill 78, it is assumed that eHealth Ontario will be the first entity to be named as such.

EPHIPA previously reached second reading but died on the Order Paper when the legislature dissolved on May 2, 2014. In a news report released on June 10, 2015 by the Ontario Ministry of Health and Long-Term Care, the government has announced its intention to re-introduce a number of the protections to electronic and other PHI, as presented in 2013 through EPHIPA. While it is not completely clear when the new amendments will be put forth, and in what form, below are some of the key amendments from EPHIPA that, if and when re-introduced, have implications for health care providers and prescribed organizations.

Key EPHIPA Provisions:

Prescribed Organizations

One of the main focuses of EPHIPA is the introduction of "prescribed organizations" as essentially the service providers of the electronic health record database and its related systems. A similar concept does exist in the current regulations made under PHIPA in the form of "health information network providers" ("**HINPs**"). HINPs are defined in the general regulation to PHIPA as a "*person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians*." The regulations under PHIPA prescribe minimum standards that are applicable to HINPs including obligations relating to security of PHI, notification of breaches of confidentiality and logging and documenting of data accesses. As well, a HINP must enter into a written agreement with each health information custodian concerning the services provided to the custodian that: a) describes the services that the provider is required to provide for the custodian; b) describes the administrative, technical and physical safeguards relating to the confidentiality and security of the information; and c) requires the HINP to comply with PHIPA and its regulations.

The EPHIPA provisions relating to prescribed organizations are in the same spirit as those relevant to HINPs and build upon the framework that is already in place. However, the EPHIPA provisions applicable to prescribed organizations contain more robust requirements, including a tri-annual audit of the prescribed organization's privacy and security framework by the Information and Privacy Commissioner.

*Collection, use and disclosure of PHI by health information custodians ("**HICs**")*

Under EPHIPA, a HIC can provide PHI to a prescribed organization for the purposes of creating or maintaining the electronic health record, and in doing so, the HIC will not be considered to be "disclosing" PHI and the prescribed organization will not be considered to be "collecting" PHI. Disclosure is deemed to occur where a HIC, other than the HIC that originally provided the PHI to the prescribed organization, initially views, handles or deals with the PHI in the electronic health record for the first time. A HIC *collects* PHI on the initial instance on which it views, handles or otherwise deals with PHI in the electronic health record that the HIC has not provided itself to the prescribed organization. Any subsequent viewing, handling or dealing with PHI in the electronic health record by either the original HIC who provided the PHI to the prescribed organization in the first place, or a HIC that has already viewed, handled or dealt with PHI in the electronic health record, is deemed to be a "use" so long as no new or additional information is viewed, handled or otherwise dealt with. EPHIPA also specifies that the only purpose for which a HIC can collect PHI is to provide health care or to eliminate or reduce a significant risk of serious bodily harm to a person or group of persons.

Consent directives

Despite the proposed changes introduced by EPHIPA, the legislation will retain the overarching general privacy principles promulgated by PHIPA and PIPEDA, including the concepts of limited access to a patient's PHI. In particular, under EPHIPA, a patient may limit access to his or her PHI in the electronic health record by a consent directive provided to a prescribed organization. Through a consent directive, a patient may withhold or withdraw his or her consent to the collection, use and disclosure of his or her PHI contained in the electronic health record for the purpose of providing or assisting in the provision of health care to the individual. This concept is similar, with some modifications, to the "lock-box" provisions in PHIPA and like such lock-box provisions, there are circumstances under which a HIC may override the consent directive, including to eliminate or reduce a significant risk of serious bodily harm to the patient or others. However, unlike lock-box requests, EPHIPA provides that a prescribed organization is the exclusive manager of consent directives and as such, all patient requests to limit access must be made to and decided by the prescribed organization. Prescribed organizations must audit, log and monitor access to PHI that is subject to a consent directive and may override a consent directive for the purpose of notifying a HIC about potentially harmful medication interactions, so long as such notification does not reveal underlying PHI that is subject to the directive.

Mandatory reporting of privacy breaches

In the event that PHI in the electronic health record is stolen, lost or accessed by unauthorized persons, the prescribed organization must notify the HIC that provided the PHI in question. As well, the prescribed organization must notify the Information and Privacy Commissioner in writing where the prescribed organization (or someone that it has retained) has dealt with the PHI in the electronic health record in a manner that is contrary to the legislation or where there has been an unauthorized release of PHI in the electronic health record.

Increase in fines for PHIPA offences

Under EPHIPA, there is no limitation period for prosecution of offences under PHIPA. More importantly, EPHIPA doubles the monetary fines for offences committed under the legislation. For an individual offender, the fine is increased from $50,000 to $100,000 and for a corporate offender, the fine is increased from $250,000 to $500,000. If such proposed amendments are reintroduced this could significantly increase organizations' exposure for offences.

Contractual considerations

Until the proposed amendments are actually introduced, it is difficult to fully comment on the implications for all those involved in the provision of health care. However, it appears that prescribed organizations as well as

HICs may have a number of additional responsibilities that they must consider. While the amendments to PHIPA found in EPHIPA do provide a number of explicit duties and obligations applicable to parties involved in the creation, contribution and access to the electronic health record, it is still arguably important to specify and delineate these responsibilities and liabilities through contractual means.

In particular, network services agreements (as currently required for HINPs), are still relevant in that they should still be used to set out the specific services to be provided by a prescribed organization as well as identify the responsibilities and allocate risk between the prescribed organization and participants in the electronic health network. Additionally, there continues to be a need for data sharing agreements since these agreements address the exchange and sharing of PHI between participants of a network, typically excluding the HINP (or prescribed organization).

Conclusion

It has become apparent that the use of electronic health records and the changing health care delivery model, while extremely beneficial and efficient in many ways, present a greater risk of unauthorized access, use and disclosure of PHI. As Brian Beamish, the Ontario Privacy Commissioner, stated "*patients who don't have faith in the security and privacy of electronic health records may not provide full and accurate information to their health-care providers – and that could impact the health care they receive*." As such, amendments to PHIPA are necessary and overdue, and the provisions first introduced by EPHIPA were meant to protect Ontarians' PHI as well as provide greater oversight and compliance. While the actual amendments have yet to be released, it is important for HICs and prospective prescribed organizations to consider the types of changes to health privacy laws that will likely be introduced in the near future, and prepare for the additional responsibilities that will result.

by Ratika Gandhi

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.

© McMillan LLP 2015