David Young Law
Compliance Bulletin

May 2020

COVID and other privacy developments – Ontario

On March 25 the Ontario Government introduced and had passed into law Bill 188, its *Economic and Fiscal Update Act, 2020*, more accurately understood as its initial pandemic response legislation. While the Act includes amendments to a number of statutes targeted to address the COVID-19 pandemic, it contains significant amendments to the province's health and public sector privacy laws - which may serve that objective - but potentially have more far-reaching implications.

Significantly, the amendments represent a precedent-setting extension of the application of Ontario's privacy laws outside of the "public interest" sector.

On one hand, these amendments may facilitate private sector organizations to develop and maintain electronic health record (EHR) systems independent of the current health sector. On another level, they enable private sector entities to collect and perform analyses of both health and non-health related public sector information, on their own behalf and not as service providers to government.

The breadth and scope of these amendments suggest that they were not developed entirely as an urgent response to the COVID crisis but also as reflective of the potential future involvement of private sector entities in the management and analysis of public interest personal data. While the amendments may be warranted in the context of the response to COVID, they could have longer-term impact regarding the respective roles of the public versus private sectors in relation to the stewardship of personal information in Ontario.

PHIPA - privacy-protective enhancements

The health-related amendments include certain privacy-protective enhancements. However, a closer examination suggests that in other respects they may have unintended consequences.

The amendments to PHIPA[1] enacted by Bill 188 encompass a number of privacy protective enhancements to the province's personal health information oversight framework. Most significantly, they provide for a new power for the Information and Privacy Commissioner (IPC) to impose administrative monetary penalties (AMPs) for breach of the Act, in an unlimited amount, subject only to guidelines to be prescribed by regulation. Additionally, they increase potential fines for offences under the Act (which are prosecuted by the Attorney General, not the Commissioner) to $200,000 for individuals and $1,000,000 for corporations.[2] The power to

[1] *Personal Health Information Protection Act, 2014*.
[2] From $100,000 and $500,000 respectively.

impose AMPs is a first for a privacy regulator in Canada and may point a direction for anticipated amendments to the federal privacy law, PIPEDA.[3]

The amendments also provide a requirement for health information custodians that maintain EHRs to have electronic audit logs for their databases, available for inspection by the IPC at any time. Audit logs must include up to date records of all accesses to a database including the time, particulars of the relevant information, and the identity of the person or persons involved in the access. Recommended by the IPC as a best practice to address unauthorized access to patient records (such as employee "snooping"), the audit log provision now will be legislatively mandated.[4] While such logs are standard for large organizations such as hospitals, the requirement may pose challenges for smaller entities such as family health teams and as such may require a transition period to full adoption.

Finally, the amendments introduce a prohibition against using de-identified information to identify an individual except as permitted by the Act. Such a prohibition, while implied under the law, is a significant added lever - enforceable by sanctions - in the toolbox of protecting such information from improper use.

Consumer Electronic Service Providers

Separate from the noted privacy-protective enhancements to PHIPA are amendments that address and, arguably, support the expansion of private sector health databases. A new category of regulated entity is identified - "Consumer Electronic Service Provider". Consumer electronic service providers (CESPs) are defined as persons who provide 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. Essentially, these are private sector providers of medical record databases to which individuals have subscribed for purposes of maintaining an accessible electronic record of their PHI. CESPs will be subject to rules prescribed by regulation, presumably distinct from those governing health professionals.

The most prominent current Canadian example of a CESP is TELUS Health.[5] However any non-public sector database holding personal health information, including those created for simply health and wellness purposes[6] or potentially even research, through collection of PHI directly from individuals will be subject to the new oversight provisions. Significantly therefore, the application of PHIPA is extended to entities currently outside of the health care sector that hold PHI, not as a service providers to the sector, but as data collectors in their own right as vendors of a consumer-oriented service.

This extension of the application of PHIPA to a potentially diverse group of health information providers appears on first analysis to be duplicative regulation of an industry that is already subject to privacy oversight under PIPEDA. Furthermore, while the thrust of PHIPA addresses protection of information in the course of providing

[3] *Personal Information Protection and Electronic Documents Act*.
[4] See the IPC's guidance document, *Detecting and Deterring the Unauthorized Access to Personal Health Information*.
[5] Other earlier instances included Google Health and Microsoft HealthVault, both of which have been discontinued as consumer-oriented electronic databases and will refocus their database services on the professional or enterprise market.
[6] Such as Fitbit, now being acquired by Google.

health care, its extension to private sector PHI databases appears to be a departure - addressing a much narrower area of application - the provision of information services to private individuals.

The rationale for this new area of oversight arguably may be found in an important additional provision – the permission for CESPs to collect individuals' health numbers for purposes of confirming the identity of their clients.[7] It can be posited that this new permission is oriented to facilitating the accurate downloading of an individual's information from their health care provider to a CESP.

As initially enacted, PHIPA strictly limited the collection and use of health numbers to health care professionals or their service providers (including database providers) for purposes related to government funding of healthcare, including planning. An understood reason was to prevent the number becoming a multi-purpose identifier that would facilitate linking of disparate information about an individual – in other words to prevent it becoming a personal identifier.[8] However under the amendments a CESP may collect and use a health number primarily for this purpose – confirming the identity of an individual.

Under the new CESP regime the use of the health number by private sector databases has other potentially significant impacts. What comes to mind is the enhanced ability for such entities to align with existing health (mostly public-) sector databases. Such databases are closely regulated under PHIPA's "HINP" rules.[9] It is unlikely that CESPs will be subject to such rigorous requirements. However a CESP, as a private sector, consumer-enabled, database may be able to align with the existing public sector systems through the health number, with the potential to develop a single EHR for a patient, for all care instances, province-wide. Such a private sector system could have the result of replicating, if not supplanting, some or all of the roles of the current public sector databases. It is not clear whether this is a policy direction of the government.

FIPPA amendments – Extra-Ministerial Data Integration Units

The second area of privacy-related amendments made by Bill 188 address the creation of "extra-ministerial data integration units" under the province's public sector privacy law, FIPPA.[10] The amendments also provide for a new category of "prescribed entity" under PHIPA[11] that will encompass these extra-ministerial ministerial data integration units.

It will be recalled that a year ago, significant amendments were made to FIPPA providing for data sharing among government ministries and other public sector entities for purposes of analysis and planning. Such data sharing

[7] The "health number" is the number assigned to an insured person under the Ontario Health Insurance Plan (OHIP).
[8] See: *Guide to the Ontario Personal Health Information Protection Act*, Perun, Orr and Dimitriadis, Toronto, 2005.
[9] See PHIPA Regulation, s. 6 which stipulates compliance requirements for "health information network providers".
[10] *Freedom of Information and Protection of Privacy Act*.
[11] Organizations designated by regulation that are permitted to collect PHI for purposes of health data research, such as ICES (formerly known as the Institute for Clinical Evaluative Sciences) and Cancer Care Ontario.

may involve the collection of personal information previously provided to government for other purposes and the linking of such information with other government databases.

A rigorous compliance regime is provided for data integration including the establishment of processing standards, de-identification to the extent possible, and oversight and approval of procedures by the IPC. This new authority to conduct such data integration operations was required since the otherwise applicable provisions of FIPPA limit collection and use of data to purposes authorized under specific program legislation or to uses directly related to such purposes. The provisions enable use of data for any resource allocation, planning or evaluation purposes by the new integration units, as designated by regulation.

When enacted last year, the data integration provisions contemplated analysis operations being conducted *within government entities* (ministerial and inter-ministerial data integration units). However Bill 188 establishes a new category of "extra-ministerial data integration unit", to operate *outside of government*, but having all the authorities to conduct data collection and analysis assigned to the intra-governmental units. Such units could be for-profit or non-profit entities.

One of the potentially significant impacts of the amendments - particularly in the context of pandemic response - is the extension of the ability to perform data integration by prescribed health research entities such as ICES and Cancer Care Ontario. Such a role is contemplated within both the PHIPA and the FIPPA amendments. To this end, an extra-ministerial data integration unit can only qualify for health data analysis if it is a prescribed entity and meets the relevant compliance requirements, including being subject to three-year reviews by the IPC. It has been suggested that a rationale for in effect qualifying prescribed entities as also extra-ministerial data integration units is to allow them the additional scope to perform analyses with data from diverse sources, for which they have been constrained to date.[12]

One can understand the urgency in the context of the current pandemic crisis to marshall resources both within government and outside of it to conduct research and develop strategies. Clearly, leveraging the technology and expertise available within the private sector is critical. However apart from the research function provided by prescribed entities, it is not clear that any such operations require the *acquisition of public sector data* by a private sector organization in its own right, as opposed to the more limited authority to *process such data on behalf of* a public sector entity. Currently, the private sector delivers diverse data analysis expertise to government through a range of service provider roles. In such roles, the ownership and ultimate control of any data remains with the public sector entity. Providing data integration analysis to government entities, including the new ministerial and inter-ministerial data integration units, would fall within such roles.

It is intended that any personal data so provided to the private sector organizations designated under this new data integration category should be de-identified to the extent possible. However it is conceivable or even likely

[12] See Teresa Scassa, "Interesting amendments to Ontario's health data and public sector privacy laws buried in omnibus bill", *Blog,* March 30, 2020.

that when the data is initially acquired by the organization it would be identifiable. Whether the data is identifiable or not, the result of these new FIPPA provisions may be the creation of significant databases, derived from public sector data, held and controlled by private sector entities.

Conclusions

Enacted within the government's legislative response to the COVID-19 pandemic, the amendments to Ontario's main privacy laws may be seen as enabling an "all hands on deck" response to the crisis. However a closer analysis suggests that they may have longer-term implications and be overly broad and even unnecessary in many respects. Furthermore they facilitate or provide for the collection and use of what may be considered "public interest" data by private sector entities. In this regard, they represent a precedent-setting extension of Ontario's public sector and related privacy legislation into the realm of private sector data protection. It is not clear whether all of these potential implications have been fully understood in adopting the amendments within the exigencies of the current crisis.

For more information please contact:
David Young 416-968-6286 david@davidyounglaw.ca
Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.