

Business

Ontario's COVID privacy amendments impact beyond public interest

By **David Young**

David Young

(June 3, 2020, 1:25 PM EDT) -- 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 legislation targeted to address the COVID-19 pandemic, it contains important changes to the province's health and public sector privacy laws — some of which may serve the pandemic response objective but potentially have more far-reaching implications.

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

The scope of these amendments suggests that beyond an urgent response to the COVID-19 crisis, they may reflect future policy directions regarding private sector entities in the management and analysis of public interest data. In this regard, 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.

Important changes to the *Personal Health Information Protection Act, 2004* (PHIPA) address and, arguably, support the expansion of private sector health databases. A new category of regulated entity is identified: "Consumer Electronic Service Provider" or CESP. Essentially, these are private sector providers of medical record databases to which individuals have subscribed for maintaining an accessible electronic record of their personal health information. CESPs will be subject to rules prescribed by regulation, presumably distinct from those governing health professionals.

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 the federal privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

However, the rationale for this new area of oversight arguably may be found in an important additional provision — the permission for CESPs to collect individuals' OHIP health numbers for purposes of confirming the identity of their clients.

As initially enacted, PHIPA strictly limited the collection and use of health numbers to health-care professionals for purposes related to government funding of health care, including planning. An understood reason was to prevent the number becoming a multipurpose identifier that would facilitate linking of disparate information about an individual — in other words to prevent it becoming a broad-based personal identifier. However, under the amendments a CESP may collect and use a health number primarily for this purpose — confirming the identity of an individual.

The use of the health number by private sector databases may result in greater ability for such entities to align with existing health (mostly public) sector databases. These databases are closely regulated under PHIPA's Health Information Network Provider rules, which govern electronic data networks maintained by the health sector. Such a private sector system could have the result of replicating or 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.

Separate from the CESP provisions, the PHIPA changes include a number of privacy-protective amendments.

The second area of the Bill 188 privacy-related amendments addresses the creation of “extra-ministerial data integration units” under the province’s public sector privacy law, the *Freedom of Information and Protection of Privacy Act* (FIPPA).

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

When enacted last year, the data integration provisions contemplated operations being conducted *within government entities*. However, Bill 188 provides for a new category of “extra-ministerial data integration unit,” to operate *outside of government*, with all the authorities to conduct data collection and analysis assigned to the intra-governmental units. A rigorous compliance regime is provided for the new non-governmental integration units including the establishment of processing standards, de-identification and regulatory oversight of procedures.

One impact of the amendments — particularly relevant in the context of pandemic response — is the enabling of prescribed health research entities such as ICES and Cancer Care Ontario to perform data integration. Such a role is contemplated within both the PHIPA and the FIPPA amendments.

One can understand the urgency in the context of the current pandemic crisis to marshal 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, as opposed to the more limited authority to *process such data on behalf of* a public sector entity.

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. It is not clear whether all of these potential implications have been fully understood.

David Young is principal at David Young Law, a privacy and regulatory counsel practice in Toronto.

Photo credit / Firm ISTOCKPHOTO.COM

Interested in writing for us? To learn more about how you can add your voice to The Lawyer’s Daily, contact Analysis Editor Richard Skinulis at Richard.Skinulis@lexisnexis.ca or call 437- 828-6772