Major access to information and privacy reform comes to Ontario

April 06, 2026

Bill 97 (the *Plan to Protect Ontario Act (Budget Measures), 2026*) will introduce significant amendments to Ontario's freedom of information and privacy framework by updating both the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). For municipal institutions, school boards, colleges and universities, hospitals, and Crown agencies, these reforms are best understood as a legislative response to sustained operational pressure under the existing access and privacy regime.

Institutions across these sectors are managing increasing request volumes; broader and more complex electronic records; repeat, overlapping and AI-driven requests; and heightened expectations around speed and completeness – often without additional resources or structural support. Bill 97 reflects an acknowledgment that the previous framework, while well-intentioned, was increasingly difficult to administer consistently and defensibly. Similar reforms in other provinces suggest a broader policy trend toward access regimes that remain principled but are better aligned with modern institutional realities.

We have summarized the Bill 97 reforms in this Insight. Bill 97 has been released in tandem with two important new regulations under the *Enhancing Digital Security and Trust Act, 2004*. For our commentary on these bills, please see Ontario introduces cyber and educational technology regulations.

Timelines that better reflect institutional realities

Bill 97 will recalibrate statutory timelines by shifting most deadlines under FIPPA and MFIPPA to business days rather than calendar days. The basic period for answering a request will increase from 30 days to 45 business days. For institutions operating with limited freedom of information (FOI) staffing, shared privacy roles, or decentralized records management, this change alone significantly reduces artificial deadline pressure.

The legislation will also expand institutions' ability to extend timelines, including the option for a second extension in defined circumstances, such as unexpectedly large record volumes or unforeseen consultation or staffing challenges. These changes are

particularly important for school boards, municipalities, and health organizations that routinely receive broad, multi-year, requests for large volumes of electronic records.

Staged access plans: A practical tool for large requests

The introduction of staged access plans will be one of the most operationally significant reforms in Bill 97. Institutions will be able to respond to large or complex requests by proposing a structured, phased approach to search, review, and disclosure.

An institution will be permitted to propose a staged access plan where:

- Searching for records would unreasonably interfere with employees' regular duties;
- The request is "overly broad" due to the period covered;
- The volume of records and preparation effort would unreasonably interfere with operations; or
- The requester has made multiple requests that, taken together, unreasonably interfere with operations.

The plan must be set out in writing and must:

- Divide the request into distinct categories of records, identifying the areas of the institution to be searched; and
- Establish a schedule indicating whether and when access decisions will be made for each category, and when records (or portions) will be disclosed or produced.

Requesters will have 30 business days to respond by either accepting the plan, proposing amendments, or narrowing the scope of the request, otherwise the requester may appeal.

A requester may appeal the initial decision to propose a plan, and the first amendment to a plan, to the Information and Privacy Commissioner (IPC). The requester's duty to respond is mandatory. If the requester does not respond appropriately within the statutory timeframe (and does not appeal where permitted), the request will be deemed abandoned.

Once a plan is proposed, the statutory response clock pauses while the requester responds. A response will restart the clock, and the institution can propose another plan so long as the response clock has not been exhausted.

Institutions may amend a staged access plan as needed. While the initial proposal – and the first amendment only – is subject to appeal, subsequent amendments are not appealable, giving institutions significant flexibility to adjust plans in response to operational realities.

Fee estimates as scope and timing controls

Bill 97 tightens, standardizes, and aligns fee estimate rules with staged access response-clock processes. Specifically:

- Institutions will be expressly required to inform requesters of their right to request a fee waiver;
- Institutions will be expressly required to issue fee estimates before the response clock expires;
- Fee estimates will pause the response clock.

In short, fee estimates will operate as a more formal, procedural control point, aligned with staged access and response-clock mechanisms.

Politically sensitive records (FIPPA)

The amendments will add a new provision to FIPPA, such that FIPPA will no longer apply to records in the custody or under the control of a minister, a minister's office, or a parliamentary assistant acting in that capacity. Once in force, the amendments will generally exclude ministerial and parliamentary assistant records from FIPPA, except for records under ministerial control that are also in the custody or control of an institution, which will continue to be subject to FIPPA.

Exclusion for cybersecurity -sensitive records

Both FIPPA and MFIPPA will exclude, and therefore not apply to, records "prepared or collected under" the *Enhancing Digital Security and Trust Act, 2024* (EDSTA). This exclusion will apply to the following such records:

- Records containing the names of employees designated as primary points of contact for ensuring cybersecurity within each public sector entity and their alternates.
- Assessments or evaluations of a public sector entity's status or progress with respect to cybersecurity or summaries of such assessments or evaluations.
- Records containing the names of software applications that have been purchased or otherwise acquired by school boards, that are owned or operated by third parties, and that are authorized to access a student's personal information.
- Any other records the disclosure of which could reasonably be expected to compromise cybersecurity for a public sector entity.

For institutions increasingly targeted by ransomware and other cyber threats – particularly school boards and hospitals –, this change will provide powerful statutory backing by removing specified security sensitive records from the public right of access. The protection is implemented by way of a jurisdictional-limiting exclusion, which invites a more institution-favourable analysis should exclusion claims be challenged.

The exclusion hinges on a statutory linkage to EDSTA. Questions may arise as to whether a record must be explicitly required or generated under EDSTA authority, or, alternatively, merely related to cybersecurity work undertaken in response to EDSTA obligations.

Aligning MFIPPA privacy governance with FIPPA

When FIPPA was amended in 2025 to require mandatory breach reporting and notification, mandatory privacy impact assessments, and to otherwise modernize the FIPPA privacy compliance regime, MFIPPA was not likewise amended. Bill 97 rectifies this imbalance by amending MFIPPA to:

- Introduce mandatory privacy breach reporting to the IPC, and notification to affected individuals where there is a real risk of significant harm;
- Require municipal institutions to prepare privacy impact assessments (PIAs) before collecting personal information, and to update PIAs where there are significant changes to use or disclosure;
- Impose an express statutory duty to implement reasonable administrative, technical, and physical safeguards to protect personal information;
- Require municipal institutions to maintain records of privacy breaches and to report breach statistics annually to the IPC;
- Expand the IPC's oversight role, including authority to review institutional information practices where there are reasonable grounds to believe MFIPPA has been contravened, and to make compliance orders; and
- Introduce whistleblowing protections, permitting individuals to confidentially notify the IPC of suspected contraventions of MFIPPA.

These changes will significantly expand MFIPPA institutions' operational privacy obligations, increase the IPC's supervisory role, and require a more structured, proactive approach to privacy governance, breach response, and risk management across the municipal public sector.

Conclusion and practical next steps

Bill 97 will bring both blessings and burdens for Ontario institutions.

On the access to information side, the reforms acknowledge the operational strain institutions have been under for years, and provide meaningful relief through longer timelines, staged access plans, clearer fee estimate mechanics, and targeted exclusions. Properly used, these tools should help institutions manage volume, complexity, and expectations in a more sustainable way.

At the same time, the bill does not simply reduce obligations. For municipal institutions, the new MFIPPA privacy governance provisions introduce a more formal, proactive compliance framework: mandatory breach reporting and notification, documented privacy impact assessments, explicit safeguard obligations, breach record keeping, and enhanced IPC oversight. These requirements will require focused work to implement, at a moment when many institutions are facing tight budgets, staffing constraints, and competing operational priorities.

Practical steps institutions should be considering now include:

- Reviewing and updating FOI procedures to reflect business day timelines, staged access plans, extensions, and fee estimate pauses;
- Training FOI and program staff on when and how to use staged access plans and extensions defensibly;

- For municipal institutions, assessing current privacy practices against the new MFIPPA requirements, including PIAs, breach response, safeguards, and record keeping;
- Identifying pragmatic, proportionate ways to meet new obligations without over engineering processes or duplicating effort.

Bill 97 creates an opportunity for institutions to reset both access and privacy practices in a more sustainable way. With thoughtful planning and proportionate implementation, the reforms can reduce pressure where relief was clearly intended, while strengthening privacy governance in a way that is manageable rather than overwhelming.

By

Daniel J. Michaluk, Marc Vani, Avital Sternin

Expertise

Cybersecurity, Privacy & Data Protection, Health Law, Government & Public Sector

---

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary
Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa
World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver
1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal
1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749