

October 8, 2026

ATIPPA Statutory Review Committee
2nd Floor, Beothuck Building
20 Crosbie Place
St. John's, NL
A1B 3Y8
ATIPPAReview@gov.nl.ca

Re: Review of Access to Information and Protection of Privacy Act, 2015 (ATIPPA, 2015)

1. About WorkplaceNL

WorkplaceNL administers Newfoundland and Labrador's mandatory, employer-funded, no-fault workplace injury insurance system. The system rests on the Meredith Principles: no-fault compensation, collective liability, security of payment, exclusive jurisdiction, and an independent board that is autonomous and financially independent of government.

WorkplaceNL revenue comes from employer assessments, reimbursements and administrative fees from self-insured employers, and investment income. Every hour spent on statutory compliance is an hour funded by the province's employers.

We provide coverage to approximately 98 per cent of the province's workers, serving more than 17,000 employers and roughly 230,000 workers.

Our operating environment is unusual in one respect that shapes this submission: we are subject to ATIPPA, 2015 and *Personal Health Information Act* (PHIA). Most of our records relate to workplace injury claims and involve personal health information, which is currently governed by PHIA as WorkplaceNL is a designated custodian under s. 4 of that Act and s. 6 of ATIPPA, 2015 gives PHIA precedence in those circumstances. However, records that are not part of a claim such as file information about employers, corporate records, and employment records, are governed by ATIPPA, 2015.

Managing the same function under two statutes with materially different rules gives us a practical view of where the two Acts diverge without good reason. That is the basis for our primary recommendation below.

2. Privacy Breach Management (Terms of Reference, item 5)

2.1 The current reporting threshold under s. 64(4) is not calibrated to risk

Section 64(4) of ATIPPA, 2015 requires the head of a public body to inform the Office of the Information and Privacy Commissioner (OIPC) of any breach involving the unauthorized collection, use or disclosure of personal information. The obligation sets no threshold. A misdirected email containing a single name is reportable on the same terms as a large-scale unauthorized disclosure of sensitive records.

This is inconsistent with the rest of s. 64. Where the Act deals with notifying the *individual*, it applies a harm-based test: s. 64(7) removes the notification obligation where the head reasonably believes the incident does not create a risk of significant harm; s. 64(8) defines significant harm; and s. 64(9) sets out the relevant factors, being the sensitivity of the information and the probability of misuse.

The Act therefore already contains a materiality test, but it does not apply to reporting to the OIPC.

PHIA takes a more practical approach. Section 15(4) requires a custodian to inform the OIPC only where the custodian reasonably believes there has been a *material breach*, and s. 5 of the Personal Health Information Regulations defines the relevant factors:

- the sensitivity of the information,
- the number of people affected,
- whether the information has been or will be misused, and
- whether the cause or pattern of breaches indicates a systemic problem.

The result is that WorkplaceNL applies two different reporting standards to incidents that are often functionally identical, differing only by whether the record that was breached happened to sit inside or outside a claim file.

Where the OIPC oversight is genuinely valuable is in cases involving sensitive information, multiple affected individuals, deliberate misuse, or a systemic or recurring cause. Those are precisely the cases captured by the PHIA materiality test.

Recommendation 1: Amend s. 64(4) to require reporting to the Commissioner only where the breach is material, using criteria equivalent to those in s. 5 of the Personal Health Information Regulations and consistent with the existing risk-of-significant-harm framework in ss. 64(7) to (9).

2.2 Privacy Breaches at WorkplaceNL

WorkplaceNL maintains a log of both privacy breaches and privacy *incidents*- situations where no breach occurred under the legislation but where an opportunity for improvement was identified.

Approximately 94 per cent of breaches at WorkplaceNL are caused by human error: a typographical error in an email address, incorrect fax number was entered, an attachment sent to the wrong recipient. These are almost always contained quickly, involve one recipient and one individual's information, and carry no realistic prospect of misuse.

We actively encourage staff to report these situations, because internal reporting is what allows us to target training and improve workflows.

2.3 Limits of Breach Reporting

If the objective of s. 64(4) is data collection, building a provincial picture of breach volume and type, the resulting data is not reliable. In their latest annual report the OIPC reported 162 breaches under ATIPPA and 32 under PHIA. Public bodies vary widely in how they identify, characterize and count breaches, and in the maturity of their internal

reporting cultures. A public body that reports diligently appears worse than one that does not. Aggregate figures drawn from this base cannot meaningfully support comparison or analysis.

If the objective is reducing the number or severity of breaches, the OIPC's role at the incident level is limited. The public body is responsible for training staff, designing workflows, and configuring systems and controls. For a low-risk human-error breach, the corrective action is identified and implemented by the public body often before the report is even filed. External reporting adds an administrative step with no impact on the outcome.

Reporting singular privacy breaches to the OIPC that pose no risk to individuals and require no further action from the OIPC, the public body or the individual, does not appear to add additional impact to the prevention of privacy breaches. Therefore, equal impact could be achieved by reporting them on a regular interval rather than per-breach.

Recommendation 2: Amend the Act to require public bodies to report summary breach statistics periodically (ex. quarterly, annually) to the OIPC.

3. Access to information provisions (Terms of Reference, item 2)

3.1 Request Volume

WorkplaceNL has seen a substantial increase in access to information requests:

Fiscal year	Requests received
2023–24	6
2024–25	14
2025–26	53
2026–27, to September 2026	31

Throughout this period WorkplaceNL maintained a 100 per cent response rate and a 100 per cent on-time rate.

That would not have been possible without the assistance of the ATIPP Office and the OIPC. The OIPC in particular has been consistently responsive and has a strong record of making decisions within legislative timelines, including on extension and disregard applications where our ability to respond on time depended on a decision within days. We want to acknowledge that contribution to the functioning of the system.

3.2 Non-Responsive Applicants

ATIPPA, 2015 does not provide a clear mechanism for closing a file where an applicant does not respond to a request for clarification.

Section 13(1) obliges us to make every reasonable effort to assist an applicant. Where a request is unclear, coordinators go about seeking clarification. But the Act contemplates abandonment only in the narrow context of a cost estimate under s. 26(2), and the s. 16(1) clock continues to run regardless of whether the applicant has responded. The available options are to apply for an extension under s. 23, which must be done within 15 business days of receipt, or to apply to disregard under s. 21, which must be done within 5 business days of receipt.

In practice, some applicants are often busy professionals who intend to respond and simply have not. In three instances this year, applicants have replied to requests for clarification outside of the 15 day allowance for applying for a time extension. Public bodies are left choosing between processing an overly broad request at unnecessary cost, refusing a request the applicant may have narrowed, or providing a response outside of statutory timelines.

Recommendation 3: Amend the Act to provide that where a public body has made reasonable efforts to obtain clarification and the applicant has not responded within a defined period, the time limit under s. 16(1) is suspended,

or the request may be treated as abandoned after a further defined period, subject to written notice to the applicant and a right to reactivate the request.

3.3 Requests Prepared with AI Assistance

Applicants are increasingly using generative AI tools to prepare access requests and related correspondence. The current statutory framework is not structured with this technology in mind.

The pattern we have observed:

- **Length without specificity.** Our largest request in the past year ran to approximately 1,500 words where roughly 50 words would have identified the same records. Length of this kind does not improve the description of the request, rather it obscures it.
- **Scope drift between exchanges.** Publicly available AI tools do not reliably carry context between sessions. In one case this year, follow-up correspondence resulted in further alteration of the request, changing scope and parameters mid-process.
- **Correspondence that does not respond to the question asked.** Clarification exchanges can produce replies that are fluent but non-responsive, extending the exchange without narrowing the request.

The underlying issue is the applicant's unfamiliarity with the records, the business processes of the public body, or the access to information process.

The consequence is more processing hours, less efficient processing, and applicants who are less likely to receive the records they wanted.

However, WorkplaceNL also recognizes the benefits that the technology can provide applicants, including overcoming language barriers. Further, the use of this technology alone should not preclude an applicant from submitting a request. The issue is that the scope of the requests prohibits coordinators from processing them.

Recommendation 4: The committee explore formal guidelines and standards with regards to the scope, complexity, and clarity of individual requests.

WorkplaceNL would welcome the opportunity to discuss any of the above. Please direct questions to Blaine Edwards, Privacy Analyst, 709-778-6983.

Yours truly,

Rebecca Phillipps, B.A. LL.B
General Counsel & Corporate Secretary
WorkplaceNL