How is your REB’s privacy muscle?

February 04, 2026

Canadian health privacy statutes grant research ethics boards (REBs) a significant power to dictate how personal health information can be used in approved research projects. Attached to that power are duties to ensure that REB approvals adequately protect the privacy of individuals.

Statutes protect health privacy and enable research

Health privacy statutes both protect personal health information and enable research.

They protect personal health information as being among the most sensitive types of personal data. The rules in health privacy statutes are strict. For example, express consent is generally required to use personal health information for purposes unrelated to the provision of health care.

They also provide health information custodians and researchers the ability to use personal health information for research without consent. However, use of personal health information (rather than de-identified information) for research purposes must be “necessary” and express consent must be “impractical.” There are other requirements that vary by province.

The statutes reflect important policy: health research serves the public good, and requiring individual consent for every use and disclosure of personal health information would impede research and scientific discovery.

Statutes respect academic freedom and institutional autonomy

Health privacy statutes also respect academic freedom and the autonomy of higher education institutions. They do so by assigning to REBs the power to decide whether the use of personal information is necessary and whether obtaining express consent impractical. These boards are independent committees of experts and community members that review, approve, and monitor research involving human participants to ensure it meets ethical, scientific, and regulatory standards.

REBs are given a statutory power and duty to evaluate the privacy risks associated with research projects on a case-by-case basis, and consider, among other things, whether the privacy risks are properly balanced against the research being conducted and whether the risks are appropriately mitigated. They have significant discretion in exercising this power and duty. The regime is one of self-governance, and approval decisions by REBs cannot be second-guessed by privacy regulators.

Researchers rely on REB approvals, answer to custodians and trustees

Although they enable research, the primary focus of health privacy statutes is on the regulation of health care professionals – called health information custodians or trustees. Custodians and trustees can either disclose personal health information to a researcher with express consent or based on the approval of an REB. There are rules governing how researchers must present REB approvals to custodians and trustees in every province.

In Ontario, for example, section 44 of the *Personal Health Information Protection Act*, 2004 (PHIPA) governs non-consensual disclosures of personal health information to researchers. To comply, custodians must receive a written application that supports the disclosure of personal health information, a copy of the approved research plan, and a copy of the REB decision that approves the research plan. They must also enter a data sharing agreement with the researcher by which the researcher agrees to “comply with the conditions and restrictions, if any, that the custodian imposes relating to the use, security, disclosure, return or disposal of the information.”

This is a key point in the research workflow; researchers need to obtain data while satisfying custodians that privacy risks will be appropriately mitigated. Custodians must satisfy themselves that approval has been granted and enter a binding agreement that renders researchers accountable to them. Although disclosing custodians do not govern researchers in any legal sense, if a researcher suffers a privacy breach, the researchers must notify all disclosing custodians, not the affected individuals.

Statutes prescribe a framework for evaluating research plans

As explained, the non-consensual disclosure of personal health information rests entirely on the REB's approval of the research plan. Although health privacy statutes afford significant latitude to REBs, they have a statutory duty to consider certain factors when evaluating a research plan. In addition to considering whether the use of personal health information (rather than de-identified information) is "necessary" and whether obtaining express consent is "impractical," statutes may impose other mandatory considerations. In Ontario, for example, an REB is required to consider "whether, at the time the research is conducted, adequate safeguards will be in place to protect the privacy of the individuals whose personal health information is being disclosed and to preserve the confidentiality of the information."

Given their statutory duty to engage in privacy analysis and consideration, REBs ought to document their consideration and reasoning. This is an express requirement in

Alberta, Ontario, and PEI. Ontario, for example, requires REBs to “provide to the researcher a decision in writing, with reasons, setting out whether the board approves the plan, and whether the approval is subject to any conditions, which must be specified in the decision.”

A bottom-line approval decision will not satisfy this requirement and will render the “conditions” that bind the researcher vague. Is the researcher to adopt all of the safeguards set out in the application for approval or just some of them? Has the researcher set out the safeguards clearly enough to support REB understanding? Has the REB deemed all such safeguards to be adequate without clarification, augmentation, or enhancement?

Although the obligations arising out of health privacy statutes are particular and subject to privacy regulator oversight, we note that they are generally aligned with obligations under the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS2) if the research considered is funded by the Tri-Council agencies (CIHR, NSERC, SSHRC). TCPS2 requires that REBs function impartially and provide reasoned and appropriately documented opinions and decisions for both approvals and denials. Importantly, an REB **must detail** its decisions when exercising the power to waive consent requirements.

A thorough REB evaluation fosters institutional trust

Each time an REB approves a research plan that authorizes the use of personal health information for research purposes, it is representing that the use of personal health information for the project is appropriate and that the personal health information will be adequately safeguarded. It is also exercising a trust placed in it by the institution, the research community, and the public.

A robust privacy analysis, set out in written decisions, is not only required by privacy statutes, but is also the mechanism through which REBs uphold that trust. Clear written decisions that transparently demonstrate responsible handling of key privacy issues are protective of the REB, supportive of researchers and research, and will help keep data flowing to support scientific discovery.

The bottom line

The power vested in REBs under Canadian health privacy statutes is substantial and important. Exercising this authority requires an informed, proportionate, and documented privacy analysis.

Institutions and their REBs that treat privacy review as an important exercise in legal and ethical judgment will be better positioned to defend their decisions and fulfil the duties imposed on them by Canadian law. They can enhance this ability by providing education to members on privacy and data security principles so REB members are confident in their analysis and able to enable research while avoiding undue privacy risk.

This bulletin is intended for informational purposes only and does not constitute legal advice. The legal landscape governing research ethics and personal health information

is complex and continues to evolve. Please contact us for advice on the application of these principles to your specific circumstances.

By

Daniel J. Michaluk, Marc Vani, Avital Sternin

Expertise

Cybersecurity, Privacy & Data Protection

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

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.