How North American Privacy Frameworks Shape Real-World Evidence: A Comparison of Canada and the United States

Samantha Gorun, MRes - Associate Research Scientist

Introduction

Real-world evidence (RWE) has become central to health technology assessment (HTA), post-market surveillance, and value-based decision-making. Yet the feasibility of generating and using RWE is shaped largely by regulatory environments that govern privacy, cross-jurisdictional sharing, and data access. These frameworks determine who can access personal information, under what conditions, and with what limitations.

Variability in data-sharing policies across authorities may influence data completeness, population representation, and the feasibility of certain study designs. Additionally, jurisdictions with more restrictive policies may impose greater barriers to data use, while others may offer more streamlined access. As a result, privacy regulation becomes a structural determinant of bias, shaping not only what data can be used, but which populations are represented, how complete datasets are, and how feasible certain study designs become.

This post compares the regulatory landscapes of Canada and the United States (U.S.) and examines how privacy laws and data-governance frameworks can influence the production and use of RWE, and the limitations these structures may impose.

Privacy Frameworks in Canada and the U.S.

Canada (PIPEDA)

In Canada, data-sharing and access policies are shaped by both federal and provincial regulation. The Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's federal private-sector law, oversees the collection, use, and disclosure of personal data in commercial activities, not only in health contexts.[1] Accessing Canadian health data is further limited by the addition of provincial and territorial privacy laws which enforce extra requirements on health information custodians.[2] While PIPEDA establishes high-level federal privacy principles and Privacy Commissioners provide oversight and enforcement, access to Canadian health data is primarily governed at the provincial and territorial level.[3] Provinces and territories enact their own privacy statutes – such as Ontario's Personal Health Information Protection Act (PHIPA)[2] – which govern the collection, use and disclosure of provincial health data;[3] as a result, provincial and territorial regulatory frameworks remain strong limiting factors for conducting health research in Canada. However, while provinces and territories regulate and oversee their respective health data, decisions to access health data are usually delegated to specific prescribed entities such as the Institute for Clinical Evaluative Sciences (ICES) in Ontario,[4] or to health information custodians, such as hospitals.[3]

Additionally, some datasets – particularly those belonging to First Nations, Métis, and Inuit communities – are subject to distinct Indigenous data-governance frameworks (e.g., OCAP®), which may require separate or additional approvals for the collection, use, and interpretation of Indigenous health data.[5] As a result, such data cannot always be governed or accessed under the same governance structures as other Canadian health data.

In contrast to Canadian health privacy structures, the U.S. takes a fundamentally different approach to health-data governance.

United States (HIPAA)

In contrast to Canada's multi-level privacy framework, the U.S. operates within a fragmented, sector-specific model anchored by the Health Insurance Portability and Accountability Act (HIPAA), which – like PIPEDA – establishes privacy rules and standards governing the use and disclosure of protected health information.[6]

Additionally, under HIPAA, privacy obligations apply to "covered entities" such as healthcare clearinghouses, healthcare providers, and health plans, as well as their business associates.[7] In practice, access to health data in the U.S. may be further shaped by state-level privacy laws, introducing additional levels of regulatory complexity.

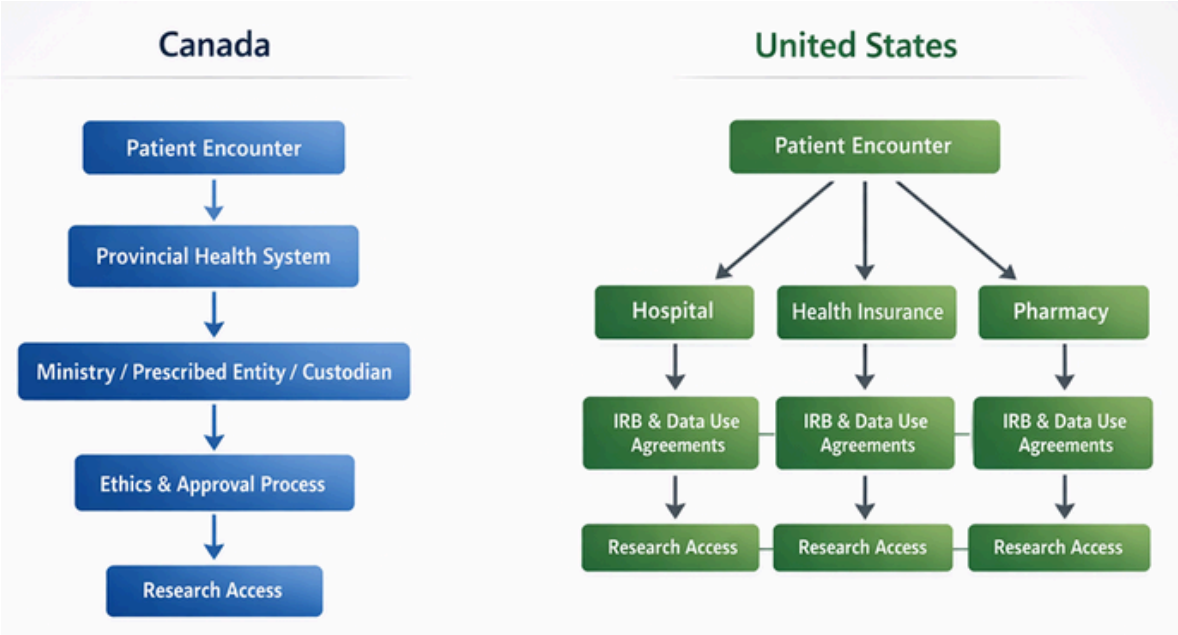
By contrast, in Canada, even after data are collected and ethics approval has been obtained, access is still subject to approval by provincial health ministries and delegated data custodians.[3] In the U.S., independent organizations collect health data and once these data are held by covered entities, HIPAA defines the conditions under which such data may be used or disclosed.[6]

Similar to Canadian Indigenous data authority and principles, in the U.S., governance of data concerning citizens of federally recognized Tribes may be subject to sovereign Tribal authority.[8] Within the data-governance and privacy structure of the U.S., conducting interstate RWE studies is further limited by this patchwork system, leading to increased legal risk, administrative complexity and burden, and uncertainty around data completeness.

Privacy Frameworks as a Structural Determinant of Feasibility

The regulatory structures across Canada and the U.S. described above translate directly into practical and methodological limitations and sources of bias for clinical research. Any clinical research, including clinical trials and observational studies using RWE, are limited by North American privacy frameworks.

Figure 1. Illustrative pathways for health data governance and research access in Canada and the U.S., highlighting differences in data centralization and access authority.



Example

Suppose a contract-research organization (CRO) is trying to use RWE to support reimbursement for a newly approved therapy. In Canada, this often means working with provincial administrative health-data. While this approach can provide highly complete data within a single province, expanding analyses across the country can be challenging. This typically requires additional interprovincial data-access approvals and in some cases, may involve separate approvals for access to Indigenous health data – directly adding to costs, time and complexity for researchers.

In the U.S., for contrast, the same question may be addressed using data directly from an integrated health system or health insurer. As a result, because these data are held by individual organizations that are governed by HIPAA rules, studies requiring access to and use of individual health data can sometimes be initiated quicker. However, such data may not include all individual health data such as those receiving care through military programs, or Indigenous populations whose data is governed under separate authorities – directly limiting representativeness of the population.

In both cases, it is important to highlight that additional bias exists within the data itself. Consent-based datasets, for example, can introduce selection bias as systematic differences may arise between individuals who opt-in to data collection versus those who choose to opt out.[9]

This example reflects a common pattern of RWE generation in Canada and the U.S. and does not capture all possible study designs or organizational arrangements.

Conclusion

Due to Canada's consent-driven and multi-custodial system, and the patchwork structure of the U.S., regulatory differences and complexity may directly increase the cost and time required to generate and utilize RWE. Obstacles often include prolonged legal review, multi-jurisdictional contracting, data-access delays, incomplete, missing or disorganized data, and inconsistent requirements within and across Canadian and American borders. For multinational studies, these delays compound, directly affecting the feasibility, timelines, and budgets of many studies. Additionally, these differences in data governance structures are not limited to Canada and the U.S. All countries offer their own specific structures to collecting, using and disclosing patient information, which adds further implications to conducting RWE studies.

References

1.Government of Canada. (2026). Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) [PDF]. https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

2.Government of Ontario. (2004). Personal Health Information Protection Act, 2004 (S.O. 2004, c. 3, Sched. A) [Statute]. https://www.ontario.ca/laws/statute/04p03/v7

3.Office of the Privacy Commissioner of Canada. (n.d.). Provincial and territorial privacy laws and oversight [Internet]. https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/

4.Institute for Clinical Evaluative Sciences (ICES). (2011, August 31). Evidence guiding health care: Report prepared for the Office of the Information and Privacy Commissioner of Ontario in respect of PHIPA requirements for review and approval of prescribed persons and prescribed entities.

5.First Nations Information Governance Centre. (n.d.). The First Nations principles of OCAP®. https://fnigc.ca/ocap-training/

6. U.S. Department of Health and Human Services. (n.d.). Summary of the HIPAA Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#who

7.U.S. Department of Health and Human Services. (n.d.). Covered Entities and Business Associates. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

8. Northwest Portland Area Indian Health Board. (n.d.). Tribal Data Sovereignty. NativeDATA. https://nativedata.npaihb.org/wp-content/uploads/2021/09/Handout-4-Tribal-Data-Sovereignty.pdf

9.Kho ME, Duffett M, Willison DJ, Cook DJ, Brouwers MC. (2009, March 12). Written informed consent and selection bias in observational studies using medical records: systematic review. BMJ;338:b866. PMID: 19282440; PMCID: PMC2769263. doi: 10.1136/bmj.b866.