



April 13, 2026

Via email: soci@sen.parl.gc.ca

The Honourable Rosemary Moodie
Chair, Standing Senate Committee on Social Affairs, Science and Technology (SOCI)
Senate of Canada
Ottawa ON K1A 0A6

Dear Senator Moodie:

Re: Bill S-5, The Connected Care for Canadians Act

We are writing on behalf of the Health, Privacy, Elder and Wills, Estates and Trust Law Sections of the Canadian Bar Association (the “CBA Sections”) regarding Bill S-5, *The Connected Care for Canadians Act*. We thank the Senate for the opportunity to comment. The CBA Sections support the Bill’s objective of facilitating health data sharing to improve continuity of care, enhance patient safety, and reduce administrative burden in an increasingly strained health care system. Achieving these objectives will depend on aligning interoperability requirements with existing federal, provincial, and territorial privacy frameworks to avoid conflicting legal obligations. The following comments identify key areas where greater clarity would strengthen the Bill.

The CBA is a national association of over 40,000 members, including lawyers, law students, notaries, and academics. Our mandate includes promoting the rule of law, improving access to justice, and advocating for effective law reform. The CBA Sections engage in legal and policy issues within their respective areas of expertise. This submission was drafted by the Health Law Section with input and review from the other above-listed CBA sections.

General Observations on Bill S-5

The CBA Sections note that Bill S-5 is directed at health information technology vendors, rather than extending obligations to health information custodians or trustees. This contrasts with the approach taken in the United States under the *21st Century Cures Act*¹ and its implementing information-blocking regulations, which apply more broadly across participants in the health information ecosystem and are intended to influence both technology providers and those responsible for the control and disclosure of health information.

The preamble of Bill S-5 sets out important objectives related to the sharing of health data, including improving patient safety and health outcomes. However, within the current Canadian regulatory framework, health information is governed by a custodial model in which health information custodians (or trustees) act as the gatekeepers of health information. They are responsible for overseeing the collection, use, disclosure, and safeguarding of health information in accordance with

¹ 21st Century Cures Act, Pub L No 114-255, 130 Stat 1033 (2016), [online](#); see also U.S. Food & Drug Administration, “21st Century Cures Act” (31 January 2020), [online](#).

applicable privacy and access legislation. In this context, while Bill S-5 may facilitate interoperability by enabling systems to communicate more effectively, it does not authorize or require the sharing of health information itself.

As a result, achieving the stated objectives of the Bill will depend not only on interoperability requirements imposed on vendors, but also on alignment with the legal and operational frameworks that govern custodians' decision-making. Additional measures, including coordination across jurisdictions and clarity regarding the role of custodians within an interoperable environment, may be required to fully realize the intended benefits of connected care. Nevertheless, Bill S-5 is an important first step toward modernizing Canada's health care systems and executing on the principles of the Pan-Canadian Health Data Charter.²

Interoperability of Health Information: The Need for Harmonization

Requiring that health information technology licensed, sold, or supplied in Canada be interoperable is a critical step toward enabling digital health systems to communicate, share, and use electronic health information safely, efficiently, and consistently. Interoperability is essential to modern health care. Fragmented systems compromise continuity of care, increase administrative burden, and create patient safety risks.

The CBA Sections understand that many of the details will be addressed in regulations. A clear statutory framework can support the secure exchange of information while respecting privacy rights and constitutional boundaries. Without clear harmonization, interoperability requirements risk creating conflicting obligations across jurisdictions and barriers to implementation.

At the same time, interoperability standards must align with federal, provincial, and territorial privacy and access laws. Consent requirements, security safeguards, research rules, and transparency mechanisms must remain central to any data-sharing framework. Omission of privacy and security-oriented requirements avoids conflicting laws in this regard, however, explicit reference to provincial and territorial privacy laws in the Bill may encourage compliance which aligns with the goal of secure interoperable systems. Robust and consistent enforcement will also be essential for the legislation to fairly achieve its intended effect.

Recommended Amendments to Definitions

Data blocking

The current definition of "data blocking" is broad and captures any "practice or act that prevents, discourages, or interferes with access to or the use or exchange of electronic health information". Greater precision is needed to avoid capturing legitimate privacy-protective practices. As drafted, the definition may inadvertently capture conduct undertaken to comply with legal obligations, discouraging appropriate privacy safeguards.

In practice, however, personal health information cannot always be disclosed in full. Health information custodians are generally required to use and disclose the least amount that may be required under provincial privacy statutes to limit or "mask" access to certain information. This may include redacting specific information or restricting access to particularly sensitive information at a patient's request, such as mental health or psychotherapy notes.

Masking is a well-established practice that supports core privacy principles. However, the broad definition of "data blocking" creates a risk that such practices could be treated as non-compliant, placing organizations in a position where compliance with provincial privacy laws may expose them to risk under Bill S-5.

² Government of Canada, *Health Canada, Pan-Canadian Health Data Charter* (12 October 2023), [online](#)

The CBA recommends that the legislation or accompanying regulations expressly clarify that lawful masking of personal health information, undertaken to comply with applicable provincial or territorial law, does not constitute data blocking.

Personal health information

The definition of “personal health information” includes “any information concerning any health service provided to the individual,” yet “health service” is not defined. In addition, the term “provided” may be interpreted narrowly and could exclude services that are referred, requested, or contemplated but not ultimately delivered. Clarification would improve certainty and avoid unintended gaps.

The CBA recommends that the definition of personal health information be expanded to expressly include information identifying health service providers. This is a common point of confusion, as health services providers may regard this as their own “personal information” rather than information connected to a patient’s care. Such an amendment would clarify that the focus of this legislation is on patient data, and is consistent with provincial legislation, including Alberta’s *Health Information Act*, and could be incorporated into the statutory definition or prescribed by regulation per section 8(a).³

Electronic health information

Given the broad application of Bill S-5 to any entity that licenses, sells, or supplies health information as a service, paired with the definition of electronic health information as meaning “electronic personal health information whether or not it has been de-identified”, there is concern that the Bill could unintentionally capture analytics, data processing, and research platforms that are not designed to enable point-of-care interoperability. For example, the types of offerings that consume de-identified or aggregated datasets for research, regulatory, safety or commercial analytics, rather than facilitating direct clinical exchange between providers. Accordingly, it is recommended that these definitions be amended in the Bill or through regulation to clarify that the core interoperability requirements and data-blocking obligations apply only to systems enabling clinical care delivery, and not to platforms used exclusively for analytics, research, quality improvement, or other secondary uses of de-identified data.

Further, the lack of differentiation between identifiable and de-identified or pseudonymized datasets and synthetic or statistically derived data could lead to consequences that negatively impact researchers and vendors without enhancing patient care.

Intellectual Property Considerations

The requirement for “complete” access and exchange of health information combined with broad anti-data-blocking provisions could create uncertainty around intellectual property requirements. For example, if “interoperability” were to be misinterpreted as requiring functional equivalence or replicability of proprietary systems. Therefore, clarification of this in the Bill or through regulations contemplated by section 5(2)(b) could be achieved by expressly affirming interoperability obligations do not require vendors to disclose or enable reverse engineering of proprietary algorithms, trade secrets, data models, derived data sets, or value-added transformations.

Impact on Elderly Persons, Substitute Decision Makers and Substitute Decision Making

Interoperable health data has the potential to improve decision-making, allowing record access across various settings, with fewer gaps or misinformation. More accurate and complete information will assist individuals and their powers of attorney (or substitute decision makers) in making health care decisions. Bill S-5 explicitly empowers patients to access their own data, which can also improve

³ *Health Information Act*, RSA 2000, c H-5, section 1(1)(i)(ii) and section 1(1)(4), [online](#).

access and decision-making for them as well as their substitute decision makers. Such data access will also allow better longitudinal insight into capacity, notes on assessments or cognitive decline. That said, the concerns of privacy and vulnerability of this age group may increase concerns of elder abuse with pressure or coercion in the misuse of the individual's medical data, which should be considered in making regulations.

Privacy and Security Considerations

Bill S-5 seeks to enable “easy, complete and *secure*” access to and exchange of electronic health information. While the term “secure” is central to the Bill’s purpose, apart from section 5(2)(a), there is no express reference to the federal and provincial privacy laws that establish requirements for security safeguards. Including such a reference to existing privacy and security requirements would reinforce the importance of privacy and security as foundational elements of interoperability.

While Bill S-5 is not intended to comprehensively regulate privacy and security, greater clarity on how safeguards will be defined and implemented would strengthen the legislative framework. Many operational details appear to be left to future regulations, which creates uncertainty at the implementation stage and raises the risk of inconsistent standards across jurisdictions and vendors.

The legislation would benefit from clearer, enforceable safeguards and a more robust framework for vetting, monitoring, and securing systems both before and after deployment, including, for example, through express reference to applicable privacy legislation.

Enforcement

Bill S-5 would benefit from clearer articulation of enforcement and accountability in a multi-jurisdictional environment. It is not clear which authority would exercise primary jurisdiction in cases involving interconnected systems, or how responsibility will be allocated where data originates in one jurisdiction but is accessed or processed in another. Clarifying whether jurisdiction is anchored to a primary system, such as the point of data origin, would help avoid gaps or conflicts in oversight. This would help prevent fragmented or inconsistent enforcement.

Many enforcement-related elements appear to be deferred to future regulations, which risks creating uncertainty for providers, vendors, and regulators. Effective deterrence from data-blocking and mandating interoperability will require penalties that are sufficiently robust to influence behaviour, along with adequate resourcing to support monitoring and enforcement.

The administrative monetary penalties and compliance verification powers contemplated by Bill S-5 should also be accompanied by clear procedural fairness protections and transparent oversight mechanisms. This includes defined review and appeal processes, as well as regular public reporting on enforcement activity. These measures would promote accountability and strengthen confidence in the regulatory framework. Given the broad definition of data blocking, it is recommended the Bill be amended to include an immunity provision to allow vendors a “good-faith compliance” defense, in circumstances where data is legitimately withheld for the purpose of complying with applicable privacy laws or where the data-blocking is at the hands of a provider as opposed to a vendor.

Conclusion

The CBA supports improved interoperability and access to health information across Canada. To ensure this is achieved securely and consistently within existing legal frameworks, the CBA recommends:

- clarifying key definitions, including “data blocking”, “personal health information”, and “electronic health information”
- expressly recognizing permissible masking practices

- clarifying the scope of interoperability and anti-data-blocking requirements
- strengthening references to privacy and security obligations
- establishing clear, enforceable baseline safeguards
- providing greater certainty regarding enforcement, jurisdiction, and accountability

We would welcome the opportunity to provide further assistance to the Committee as it continues its study of Bill S-5.

Sincerely,

(original letter signed by Yasmin Khaliq for Chairs of the contributing sections)

Sari Feferman
Chair, Health Law

Christiane Saad
Chair, Privacy and Access Law

Sara Pon
Chair, Elder Law

Amy MacAlpine
Chair, Wills, Estates and Trusts