# Brief to the Standing Committee on Social Affairs, Science and Technology

## Re: Bill S-5, *Connected Care for Canadians Act* – Privacy Legislation as a Barrier to Health Information Interoperability

**Date:** February 14, 2026

**Submitted by:** Keith Lawson, MSc, CISSP, D.Eng Student

---

## About the Author

Keith Lawson is the Chief Information Security Officer at London Health Sciences Centre (LHSC), one of Canada's largest acute care teaching hospitals, where he built and leads a managed cybersecurity services program covering 32 hospitals across Ontario. His responsibilities include security strategy, risk management, incident response, and the governance frameworks that shape how health information is protected and exchanged across organizational boundaries. Prior to his appointment as CISO, he held progressive leadership roles in IT operations, security operations, software engineering, and healthcare systems integration at LHSC and St. Joseph's Health Care London over more than two decades in the Ontario hospital system. He holds a Master of Science in Cybersecurity from Capitol Technology University and a Bachelor of Science in Computer Science from the University of Western Ontario, and is a doctoral candidate at the University of Michigan. He has published on cybersecurity in healthcare and has served as a board member of the Victorian Order of Nurses Middlesex-Elgin.

This brief is submitted in a personal capacity and does not represent the views of London Health Sciences Centre or any affiliated organization. The analysis draws on direct professional experience with the health information systems, privacy legislation, and interoperability challenges described herein.

---

## 1. Introduction

This brief is submitted in support of Bill S-5, *An Act respecting the interoperability of health information technology and to prohibit data blocking by health information technology vendors* (the *Connected Care for Canadians Act*). The objectives of the bill – establishing interoperability requirements for health information technology and prohibiting vendor data blocking – are necessary and overdue. However, the bill as drafted does not go far enough. It fails to address the most significant structural impediment to health information exchange in

Canada: the conflict between interoperability objectives and the consent-based frameworks embedded in federal and provincial privacy legislation.

This brief argues that unless Parliament simultaneously addresses the privacy law barriers that prevent health information custodians (HICs) from sharing personal health information across organizational and jurisdictional boundaries, the interoperability mandated by Bill S-5 will remain largely aspirational. HICs will continue to restrict information sharing not because of vendor lock-in or technical incapacity, but because existing privacy statutes expose them to liability for disclosures that fall outside narrowly defined consent and permitted-use provisions. The brief further argues that the bill fails to address patient access: Canadians have no enforceable right to receive their own health information in structured, usable electronic formats, and Bill S-5 does nothing to create one.

---

## 2. Bill S-5: A Necessary but Insufficient Step

Bill S-5 defines interoperability in section 5(2)(a) as technology that allows the user to "easily, completely and securely access and use all electronic health information and exchange all electronic health information with other health information technologies." This is the correct standard. The prohibition on data blocking in section 6 is equally welcome, targeting vendor practices that artificially constrain information flow.

However, section 5(2)(a) contains a critical qualification. Health information technology is interoperable only if it permits full access and exchange "unless any applicable federal, provincial or territorial law on the protection of personal health information prohibits that access, use and exchange." This carve-out is the central problem. It means the bill explicitly defers to the very privacy statutes that currently prevent interoperable health information exchange from occurring in practice. The bill mandates that vendors build systems capable of sharing data, while leaving in place the legal framework that prohibits HICs from actually using that capability.

The bill also applies in a province or territory only by order of the Governor in Council under section 7(1), and only if the Governor in Council is satisfied that the province or territory does not already have requirements that are substantially similar to or exceed those established under the Act. This opt-in mechanism, combined with the privacy carve-out, means that provinces with strong privacy protections – precisely those jurisdictions where interoperability is most constrained – are least likely to be subject to the bill's requirements.

There is a further gap. The preamble to Bill S-5 recognises that the health information of Canadians "is not easily accessible to them," yet the bill's operative provisions address only vendor obligations and system-to-system exchange. Bill S-5 creates no patient access rights, prescribes no patient-facing data standards, and does not require that interoperability specifications include mechanisms

for individuals to access, retrieve, or direct their own health information. The preamble's promise to patients is not reflected in the bill's substance.

---

## 3. The Consent Barrier under Ontario's *Personal Health Information Protection Act, 2004*

Ontario's *Personal Health Information Protection Act, 2004* (PHIPA) illustrates the problem in detail. PHIPA is the most comprehensive provincial health privacy statute in Canada and governs the conduct of health information custodians across the province.

### 3.1 The Explicit Consent Requirement

PHIPA section 18(1) requires that consent to the collection, use, or disclosure of personal health information must be a consent of the individual, must be knowledgeable, must relate to the information, and must not be obtained through deception or coercion. Section 18(3) further requires that consent must be express – not implied – in two circumstances directly relevant to interoperability:

(a) when a health information custodian discloses personal health information to a person that is not a health information custodian; and

(b) when a health information custodian discloses personal health information to another health information custodian and the disclosure is not for the purposes of providing health care or assisting in providing health care.

This means that any disclosure outside the direct clinical care relationship – including disclosures for system planning, population health, quality improvement, or cross-organizational care coordination that does not fall squarely within the "circle of care" – requires the individual's express consent.

### 3.2 The Limits of Implied Consent and the "Circle of Care"

PHIPA section 20(2) establishes the implied consent framework commonly referred to as the "circle of care." A health information custodian described in paragraphs 1, 3, or 4 of the definition of "health information custodian" in subsection 3(1) that receives personal health information about an individual for the purpose of providing health care to the individual is entitled to assume implied consent to collect, use, or disclose the information for the purposes of providing or assisting in providing health care to the individual – unless the custodian is aware the individual has expressly withheld or withdrawn consent.

This framework is narrower than it appears. Implied consent operates only among specific categories of HICs, only for the purpose of providing health care to the specific individual, and only when the individual has not exercised a consent directive. It does not extend to cross-organizational data sharing for system integration, care coordination across Ontario Health Teams where the sharing

entity is not directly involved in the individual's care, or the population-level data exchange that interoperable systems are designed to facilitate.

### 3.3 Consent Directives under Part V.1

PHIPA Part V.1 (sections 55.1 through 55.14), enacted to govern electronic health records, further compounds the problem. Section 55.6 requires that the framework for electronic health records include consent directives – mechanisms by which individuals can restrict access to their personal health information within the electronic health record. Section 55.7 provides limited consent override provisions, but these apply only in narrow circumstances such as where a health care practitioner reasonably believes that the information is necessary to eliminate or reduce a significant risk of serious bodily harm.

The practical effect is that even when interoperable systems exist and are technically capable of exchanging information, individual consent directives can prevent access at the point of care. HICs that override consent directives outside the narrow statutory exceptions face liability under PHIPA's enforcement provisions.

### 3.4 Liability Exposure for HICs

The liability framework under PHIPA is substantial and creates a rational incentive for HICs to err on the side of withholding information rather than sharing it. Section 65 provides that a person affected by a contravention of PHIPA is entitled to recover damages, including damages for mental anguish. Section 61.1 authorizes administrative penalties. Section 72 establishes offences for wilful contraventions. Sections 56 through 60 empower the Information and Privacy Commissioner to investigate complaints, conduct reviews, and issue orders.

A HIC that discloses personal health information in reliance on implied consent or a permitted-use exception, and is subsequently found to have lacked adequate legal authority for that disclosure, faces complaints to the Commissioner, administrative penalties, damage claims, and potential College regulatory proceedings. The rational response to this risk is to default to withholding information absent clear, documented, express consent for each specific disclosure – precisely the opposite of the free-flowing information exchange that interoperability is intended to enable.

Section 55.13 of PHIPA does provide protection from liability for health information custodians acting in good faith in connection with the electronic health record, but this protection is limited and does not extend to all forms of interoperable exchange contemplated by Bill S-5.

---

## 4. The Federal Barrier: PIPEDA and the Proposed Consumer Privacy Protection Act

### 4.1 PIPEDA's Consent Model

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to the collection, use, and disclosure of personal information in the course of commercial activities by private-sector organizations. In provinces without substantially similar legislation, PIPEDA governs private-sector health information custodians. PIPEDA's foundational principle is consent. Schedule 1, Principle 3 (Consent) requires that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Section 6.1 further specifies that consent is only valid if it is reasonable to expect the individual would understand the nature, purpose, and consequences of the collection, use, or disclosure.

The exceptions to consent in section 7 are limited. Section 7(3)(e) permits disclosure without consent in emergency circumstances threatening life, health, or security, and section 7(2)(c) permits use without consent for statistical or scholarly study or research where obtaining consent is impracticable. These exceptions do not contemplate routine interoperable exchange of health information across organizations for the purpose of care delivery, which is the primary use case that Bill S-5 is designed to enable.

### 4.2 Bill C-27 and the Consumer Privacy Protection Act

Bill C-27, the *Digital Charter Implementation Act, 2022*, which would have enacted the *Consumer Privacy Protection Act* (CPPA) to replace Part 1 of PIPEDA, died on the order paper when the 44th Parliament was dissolved. Had it been enacted, the CPPA would have maintained the consent-based framework while modernizing certain aspects. Section 15 of the proposed CPPA required consent for collection, use, and disclosure, and while the bill included expanded exceptions to consent in sections 18 through 39 – including exceptions for business activities, research, and emergencies – it did not include a health information interoperability exception that would have addressed the gap identified in this brief.

The inclusion of Bill C-27 in the materials under review underscores that the federal government has recognized the need to modernize Canada's privacy framework. However, neither PIPEDA as it stands nor the proposed CPPA as drafted contains provisions that would facilitate the interoperable exchange of personal health information contemplated by Bill S-5.

---

## 5. The Connecting Care Act and Provincial Integration Efforts

Ontario's *Connecting Care Act, 2019* represents an ambitious provincial attempt to integrate health service delivery through the establishment of Ontario Health and Ontario Health Teams. Section 6 sets out the objects of Ontario Health, including the promotion of health service integration and digital health, information technology, and data management services.

However, the Connecting Care Act does not override PHIPA's consent framework. The Act's provisions for permitted disclosure and collection of personal health information in section 45.1 are limited, and the Act explicitly defers to PHIPA for the definition of "personal health information" (section 1(1)) and the rules governing its collection, use, and disclosure. Ontario Health Teams that attempt to share personal health information across member organizations for the purpose of integrated care delivery remain subject to PHIPA's consent requirements, including the express consent requirement for non-care disclosures, the implied consent limitations of the circle of care, and the consent directive provisions of Part V.1.

The practical result is that Ontario Health Teams – the provincial government's primary mechanism for care integration – cannot fully realize their mandate without either obtaining express consent from every individual for every cross-organizational disclosure, or operating under the fiction that every disclosure falls within the implied consent circle of care. Neither approach is sustainable or legally defensible at scale.

---

## 6. Patient Access: The Missing Dimension

The preceding sections address barriers to information exchange between health information custodians. But Bill S-5's preamble identifies a second problem: that the health information of Canadians "is not easily accessible to them." This section examines a related but distinct gap in the current framework: patients themselves have no enforceable right to access their own health data in a structured, usable electronic format.

### 6.1 No Right to Usable Electronic Records

PHIPA section 52(1.1) grants individuals the right to request access to their records in electronic form. However, the format must either meet requirements prescribed by regulation under section 52(1.1)(a) or be specified by Ontario Health in accordance with regulations under section 52(1.1)(b). The regulation-making authority for the latter is found in section 73(1)(m.0.1). Neither mechanism has been exercised. No electronic format has been prescribed by regulation, and Ontario Health has not specified one. The right to electronic access exists in statute but is structurally hollow – in practice, custodians default to PDFs,

CDs, data on USB sticks in static, non-structured formats that cannot be imported into another provider's system, integrated into a patient-facing health application, or used for any purpose beyond reading on a screen or printing.

PIPEDA Principle 4.9 grants individuals a general right of access to personal information held by an organization. Clause 4.9.4 requires the information to be provided "in a form that is generally understandable," but this addresses comprehensibility – explaining abbreviations and codes – not electronic format. PIPEDA says nothing about structured, machine-readable, or electronic access. An organization can satisfy its access obligation by mailing a paper printout.

Bill C-27 would have introduced a data mobility right under the proposed CPPA (section 72), allowing individuals to direct the transfer of their personal information to another organization in a prescribed electronic format. The bill died on the order paper. No comparable data mobility provision exists in any Canadian statute currently in force.

Bill S-5 does not address this gap. It focuses on vendor obligations – prohibiting data blocking and mandating interoperability between clinical information systems – but creates no patient access rights and prescribes no patient-facing data standards.

### 6.2 The Custodial Model as Gatekeeper

The custodial model embedded in provincial health privacy legislation designates health information custodians – physicians, hospitals, pharmacies, laboratories – as the legal custodians and gatekeepers of patient data. This model was designed for paper records and bilateral provider-patient relationships, where a single provider held a single chart and the patient could request a photocopy.

Under this model, patients must request access through the HIC, who controls the format, timing, and completeness of the response. There is no obligation to provide data in a format the patient can use to share with other providers, integrate into personal health applications, or exercise meaningful control over. The custodial model treats patient data as institutional property to be guarded, not as personal information to be controlled by the individuals who generated it through their health encounters.

Where custodians have implemented patient-facing portals, the result has not been meaningful patient access but rather what practitioners in Ontario's e-health community have termed "portalitis": a proliferation of disconnected, custodian-specific portals that replicate in digital form the same institutional silos that characterise the paper-based model. A patient may have separate portal credentials for a hospital, a primary care practice, a laboratory, an imaging centre, and one or more specialists. Each portal displays only the information held by that custodian, in a format determined by the custodian, with no mechanism for the patient to aggregate, export, or transfer data across portals. The portal model does not solve the patient access problem – it digitises the

custodial gatekeeper model without addressing its structural limitations. A standards-based approach using FHIR APIs and SMART on FHIR, as described in section 6.4, would replace this fragmented portal landscape with a single patient-directed access model in which one application, chosen by the patient, can retrieve structured data from every custodian through a common interface.

This gatekeeper dynamic also reinforces the effects of vendor lock-in. Even if Bill S-5 succeeds in making clinical systems technically interoperable with one another, patients remain locked out. Data flows between systems at the discretion of custodians, not at the direction of patients. Without patient-facing access rights backed by enforceable format standards, interoperability serves institutions, not individuals.

### 6.3 International Comparison

The United States offers a concrete demonstration that enforceable patient access standards are achievable. The *21st Century Cures Act* (2016) and the ONC Cures Act Final Rule (2020) require certified health information technology to support standardized HL7 FHIR R4 application programming interfaces for patient access, secured through the SMART on FHIR authorization framework. The United States Core Data for Interoperability (USCDI) defines a minimum set of structured, machine-readable health data elements that must be available through these APIs. Patient-facing API access must be provided at no cost, and the information blocking prohibition extends to practices that interfere with patient access, not only system-to-system exchange. In practice, this means American patients can use SMART on FHIR-enabled applications to authenticate with their providers' systems, retrieve their health records as structured FHIR resources, and use that data in applications of their choosing – to aggregate records from multiple providers, share structured medication lists with new clinicians, or track health trends over time.

Canada has nothing comparable in force. Bill S-5 addresses vendor interoperability but does not bridge this gap. The bill's interoperability specifications under section 5(2)(b) could readily be extended to include patient-facing access standards, but as drafted they do not.

### 6.4 Available Standards: FHIR and SMART on FHIR

The standards necessary to provide patients with structured, secure, interoperable access to their own health data are mature and widely deployed internationally. Two are of particular relevance.

**HL7 FHIR (Fast Healthcare Interoperability Resources)** is a modern standard for the electronic exchange of health information, developed by Health Level Seven International (HL7). Unlike earlier health data standards that relied on document-based exchange, FHIR represents health information as discrete, structured "resources" – standardized data objects for clinical concepts such as Patient, Observation, MedicationRequest, Condition, AllergyIntolerance,

DiagnosticReport, and Immunization. FHIR resources are accessible through RESTful application programming interfaces (APIs) and are expressed in widely used data formats (JSON and XML). This design means that health data retrieved through a FHIR API is not a static document but a structured, machine-readable, computable dataset that can be imported into another clinical system, processed by a health application, aggregated across multiple sources, and acted upon programmatically.

**SMART on FHIR (Substitutable Medical Applications, Reusable Technologies on FHIR)** is an open standard that provides a secure authorization layer on top of FHIR APIs. SMART on FHIR uses the OAuth 2.0 authorization framework – the same protocol widely used across the technology industry for delegated access – to enable patients to grant third-party applications permission to access their health data from any SMART-enabled system. Under this model, a patient can authenticate with their health information custodian's system, authorize a specific application to retrieve specific categories of data, and revoke that authorization at any time. The patient controls which applications access their data, what data is shared, and for how long. SMART on FHIR thus provides a standards-based mechanism for patient-directed data access that is secure, granular, and auditable.

A third standard complements these two. The **FHIR Bulk Data Access specification** (commonly referred to as **Flat FHIR**) addresses the practical limitation that standard FHIR REST APIs are designed for individual resource retrieval – fetching a single medication list, a specific lab result, or a particular clinical note. When a patient requires a complete export of their health record – for example, when transferring to a new provider, relocating to a different province, or assembling a comprehensive personal health archive – individual API calls are impractical; a complete record may comprise hundreds or thousands of discrete resources. Flat FHIR defines a standardized asynchronous export operation that allows an authorized application to request all of a patient's data in a single operation. The output is delivered as newline-delimited JSON (NDJSON) files, where each line is a complete, self-contained FHIR resource. This format is designed to be trivially processable by modern data tools, importable into clinical systems, and suitable for downstream analysis. The export operation is secured through the SMART Backend Services authorization profile, which uses OAuth 2.0 to authenticate and authorize the requesting application. Together, FHIR, SMART on FHIR, and Flat FHIR provide the complete technical stack for patient data access: FHIR defines the data model, SMART on FHIR provides secure patient-directed authorization for real-time application access, and Flat FHIR enables complete record export and true data portability.

Together, these standards enable an ecosystem in which patients can use applications of their choosing to retrieve structured health records from every custodian that holds their data, aggregate that information in a single location, share it with new providers in a format that can be imported directly into clinical systems, export complete records when needed, and use their data in tools that

support care management, medication tracking, or chronic disease monitoring. This is not a theoretical model. It is the operational foundation of patient data access in the United States under the Cures Act Final Rule, and the major clinical information systems deployed in Canadian hospitals – including Epic, Oracle Health (formerly Cerner), and MEDITECH – already support FHIR APIs in their US implementations. The technical capability exists within Canada's installed health IT infrastructure. What is absent is any legal requirement to enable it for patient access.

The regulation-making authority in PHIPA section 73(1)(m.0.1) and the interoperability specification authority in Bill S-5 section 5(2)(b) both provide statutory vehicles through which FHIR, SMART on FHIR, and the FHIR Bulk Data Access specification could be prescribed as the standard for patient access and data portability. Neither has been exercised or directed toward this purpose.

### 6.5 Patient-Controlled Identity: W3C Decentralized Identifiers and Verifiable Credentials

The preceding standards address the format, authorization, and export of health data. A related but distinct challenge is patient identity. In the current framework, a patient's digital identity within the health system is custodian-assigned and custodian-controlled: a hospital medical record number, a patient portal login credential, a provincial health insurance number. Each custodian maintains its own identity for the patient, these identities are not portable across custodians or jurisdictions, and the patient has no control over them. When a patient moves between provinces, changes providers, or seeks care from a new institution, there is no mechanism for the patient to carry a verifiable digital identity that is recognised across systems without institutional intermediation.

**W3C Decentralized Identifiers (DIDs)**, a W3C Recommendation as of July 2022, provide a standards-based solution to this problem. A DID is a globally unique, persistent identifier that does not require a centralized registration authority and is cryptographically generated and controlled by the DID subject – in this context, the patient. Unlike traditional federated identity models where a trusted intermediary (such as a hospital or provincial authority) validates identity claims on behalf of the individual, a DID allows the individual to prove their identity through cryptographic keys they hold. The DID resolves to a DID Document containing the subject's verification methods (public keys), authentication relationships, and service endpoints. Control of the identifier is demonstrated through cryptographic proof, not through institutional permission.

**W3C Verifiable Credentials**, also a W3C Recommendation, build on this foundation. A Verifiable Credential is a digitally signed, tamper-evident attestation issued by a trusted party – in a health context, a health information custodian – to a holder, typically the patient. For example, a hospital could issue a Verifiable Credential attesting to a patient's immunization history, a pharmacy could issue one for a current medication list, and a surgeon could issue

one summarizing a completed procedure. The patient holds these credentials in a digital wallet and can present them selectively to any relying party – a new provider, a pharmacist, an insurer, an application – that needs to verify specific health information. The relying party can cryptographically verify that the credential was issued by the stated issuer and has not been altered, without needing to contact the issuing custodian. The patient controls which credentials are presented, to whom, and under what circumstances.

The relevance to the patient access problem identified in this brief is threefold. First, DIDs provide a portable, patient-controlled identity that is independent of any single custodian's systems and can persist across providers, institutions, and provincial boundaries – addressing the fragmented identity problem that currently requires patients to re-establish their identity with each new custodian. Second, Verifiable Credentials provide a mechanism for patients to carry authenticated health information that is both human-readable and machine-verifiable, enabling a model where the patient is the primary conduit of their own health data rather than a passive subject of custodian-to-custodian exchange. Third, DIDs and Verifiable Credentials complement the FHIR-based access standards described in section 6.4: FHIR provides the data model, SMART on FHIR and Flat FHIR provide the access and export mechanisms, and DIDs with Verifiable Credentials provide the patient-controlled identity and attestation layer that completes the picture of true patient data sovereignty.

The architectural model for deploying DIDs and Verifiable Credentials at scale is defined by the Trust over IP (ToIP) Foundation, which specifies a four-layer stack: Layer 1 provides decentralized trust roots through DIDs; Layer 2 enables secure peer-to-peer communication through the DIDComm messaging protocol; Layer 3 supports credential exchange using W3C Verifiable Credentials; and Layer 4 provides the governance frameworks that establish the rules, policies, and trust assurance mechanisms under which the lower layers operate. Canada has its own consensus-based framework that maps directly to this architecture. The Pan-Canadian Trust Framework (PCTF), developed by the Digital ID & Authentication Council of Canada (DIACC) with federal, provincial, and territorial input, provides a comprehensive set of conformance criteria for trusted digital identity ecosystems. The PCTF includes modules addressing digital wallets, trust registries, credentials, verified persons and organizations, and privacy – the latter explicitly aligned with the fair information principles underlying PIPEDA. The framework is actively maintained; DIACC released version 1.5 as a consultation draft, reflecting ongoing refinement based on implementation experience. The PCTF provides precisely the governance, conformance, and trust assurance layer that would be required to deploy DIDs and Verifiable Credentials in a health context in Canada. Adopting DID and Verifiable Credential standards for health information would therefore not require building a digital identity infrastructure from scratch – it would extend existing Canadian digital identity infrastructure, already grounded in the PCTF and aligned with the ToIP architecture, into the health domain.

These standards are at the highest maturity level of their respective standards bodies. Their application to health data is an area of active development internationally, and their incorporation into Canada's interoperability framework would position the country to move beyond the custodial gatekeeper model toward a model in which patients are recognised as the rightful controllers of both their health identity and their health information.

---

## 7. The Structural Problem: Privacy as a Barrier to Patient Safety

The preamble to Bill S-5 states that Parliament recognizes that the health information of Canadians is not easily accessible to them or to their health care professionals, and that this puts the safety of Canadians at risk. This is correct. The irony of the current legislative framework is that privacy legislation designed to protect individuals is, in practice, preventing the information sharing needed to ensure their safety.

A patient who presents to an emergency department with a complex medication history held across multiple providers and pharmacies cannot have that history accessed through interoperable systems if any of the relevant custodians lack clear consent authority for the disclosure. A primary care physician referring a patient to a specialist cannot electronically transmit the patient's complete record if the record contains information subject to a consent directive. An Ontario Health Team attempting to coordinate home care, hospital care, and community care for a frail elderly patient cannot share the patient's comprehensive care plan across member organizations without navigating a consent framework that was designed for bilateral custodian-patient relationships, not multi-organizational integrated care.

The privacy framework thus locks out both providers and patients. Consent barriers prevent custodians from sharing information with one another, while the absence of enforceable electronic access rights prevents patients from obtaining their own data in usable formats. The preamble's promise that Canadians will be able to access their own health information cannot be fulfilled by vendor interoperability alone – it requires that patients have a legally enforceable right to receive their records in structured, machine-readable electronic form through standardized interfaces such as FHIR APIs secured by the SMART on FHIR authorization framework, with bulk export capability through the Flat FHIR specification for complete record portability and patient-controlled identity through W3C Decentralized Identifiers and Verifiable Credentials. The standards and the technology to do this exist and are already deployed or deployable within the systems Canadian hospitals use. Without reforms on both fronts, the bill addresses the plumbing while leaving two separate taps sealed shut.

The consent framework embedded in PHIPA and PIPEDA reflects a model of health care delivery that is increasingly obsolete: the bilateral relationship

between a single provider and a single patient, where information flows are limited and identifiable. Modern health care delivery is team-based, multi-organizational, and digitally enabled. The privacy framework has not kept pace with this transformation, and Bill S-5 as drafted does not compel it to do so.

---

## 8. Recommendations

To fulfill the objectives of Bill S-5, the following amendments or complementary measures should be considered:

**8.1** Amend section 5(2)(a) to narrow the privacy carve-out. Rather than deferring entirely to all applicable privacy legislation, the bill should specify that interoperability requirements apply unless disclosure is prohibited by a privacy law provision that has been assessed against the interoperability objectives of this Act and found to be necessary and proportionate.

**8.2** Include a provision establishing a federal-provincial working group, with a defined timeline, to identify specific provisions in provincial health privacy statutes (including PHIPA) that impede interoperable health information exchange and to develop model amendments that balance privacy protection with information flow.

**8.3** Amend the bill to include a regulation-making power to establish a "trusted exchange framework" under which health information custodians that participate in an approved interoperability framework are deemed to have a permitted-use basis for disclosures within that framework, subject to appropriate safeguards including purpose limitation, minimum necessary disclosure, security standards, and audit requirements.

**8.4** Include a provision requiring that the Governor in Council, when considering an order under section 7(1), assess whether the province's privacy legislation contains provisions that would render the interoperability requirements of this Act inoperable and, if so, whether the province has taken or committed to take steps to address those provisions.

**8.5** Include a liability safe harbour for health information custodians who disclose personal health information through an interoperable system that meets the standards and specifications prescribed under section 5(2)(b), provided the disclosure is made in good faith and in accordance with the purposes of this Act. This would address the rational risk aversion that currently leads HICs to default to information withholding.

**8.6** Engage with the federal privacy law modernization process to ensure that any successor to PIPEDA (whether through a revived Bill C-27 or a new bill) includes a health information interoperability exception that permits the disclosure of personal health information without express consent where the disclosure occurs

through a system that meets prescribed interoperability and security standards, for the purpose of providing or supporting health care.

**8.7** Amend Bill S-5 to require that interoperability specifications under section 5(2)(b) include patient-facing access standards based on HL7 FHIR R4, the SMART on FHIR authorization framework, and the FHIR Bulk Data Access specification (Flat FHIR). Certified health information technology should be required to expose patient-facing FHIR R4 APIs that provide structured, machine-readable health records, to support SMART on FHIR so that patients can securely authorize third-party applications to access their data, and to support the Flat FHIR bulk export operation so that patients can obtain a complete, structured export of their records for data portability purposes. Complementary provincial reforms should require Ontario Health to exercise its authority under PHIPA section 73(1)(m.0.1) to prescribe FHIR-based electronic formats as the standard for patient access, replacing PDF and paper as the default. These standards are mature, widely implemented internationally, and already supported by the major clinical information systems deployed in Canadian hospitals. Adopting them would give patients the ability to obtain, secure, share, and use their own health data in standard, interoperable formats – and would align Canada with the patient access framework already in operation in the United States under the *21st Century Cures Act*.

**8.8** Include in the interoperability framework a provision for patient-controlled digital identity based on W3C Decentralized Identifiers (DIDs) and W3C Verifiable Credentials. Health information custodians participating in an interoperability framework under this Act should be required to support the issuance of Verifiable Credentials to patients for key health information – including immunization records, medication lists, diagnostic summaries, and care plans – in a format the patient can hold in a digital wallet and present to other providers, applications, or institutions without custodian intermediation. Incorporating DID-based identity and Verifiable Credentials would give patients a secure, portable, cryptographically verifiable health identity that persists across custodians, institutions, and provincial boundaries, and would move Canada toward a model in which patients are the primary controllers of their own health information rather than passive subjects of custodian-mediated exchange. This framework should be aligned with the Pan-Canadian Trust Framework (PCTF) and the Trust over IP (ToIP) architecture to ensure consistency with Canada's existing digital identity infrastructure and governance models.

---

## 9. Conclusion

Bill S-5 is a necessary and welcome intervention. The prohibition on vendor data blocking and the establishment of interoperability requirements address a real and longstanding problem in Canada's health information ecosystem. However, vendor behaviour is only one dimension of the interoperability problem. The

more fundamental barrier is the legislative framework governing the disclosure of personal health information by the custodians who hold it.

Unless Bill S-5 is accompanied by amendments to the privacy carve-out in section 5(2)(a) and by complementary reforms to provincial health privacy statutes such as PHIPA and to the federal privacy framework under PIPEDA, the bill will succeed in requiring vendors to build interoperable systems while leaving health information custodians unable to use them. The bill must also ensure that patients themselves can access their own health information in structured, usable electronic formats – not merely that institutions can exchange data among themselves. The bill should be amended to ensure that interoperability is not merely a technical capability, but a legal reality that serves both providers and the patients whose data it concerns.

---

*Submitted for consideration by the Standing Committee on Social Affairs, Science and Technology in connection with the study of Bill S-5.*