



Identomat

COMPLIANCE GUIDE

Healthcare Compliance in Canada

COUNTRY **Canada**

INDUSTRY **Healthcare**

LAST UPDATED **27 October 2026**

KEY REGULATORS **Information and Privacy Commissioner of Ontario · College of Physicians and Surgeons of Ontario · Office of the Privacy Commissioner of Canada**

Key takeaways

- There is no national licence for a telehealth service or health app. The clinicians who treat patients must be licensed by the regulatory college of the province where the patient is located, and patient data falls under provincial health privacy laws or the federal private-sector privacy law.
- Healthcare is not covered by Canada's anti-money laundering law, so there is no fixed list of identity documents to check. Instead, privacy statutes and professional college policies require "reasonable steps" to confirm who the patient is, and those steps must be documented.
- Online care raises the bar. In Ontario, physicians must identify the patient in every virtual visit, and pharmacists must confirm both the patient's identity and physical location every time, even for existing patients.
- Do not ask for a provincial health card as general proof of identity. In Ontario, only providers of publicly funded health services may require it, and other organisations may collect health numbers only in limited cases.
- Face matching and other biometric checks are treated as sensitive data that generally need express consent. Québec fines for misuse of personal information reach \$25 million or 4% of worldwide turnover.

Canada is open to digital health services, but there is no single regulator. Health care delivery, professional licensing and most health privacy rules are provincial; the federal government regulates drugs and controlled substances, and federal privacy law covers private organisations that are not subject to a substantially similar provincial regime. This guide uses Ontario, Québec and British Columbia as the reference provinces.

The principal authorities for a digital health business are the provincial professional colleges (in Ontario, the College of Physicians and Surgeons of Ontario and the Ontario College of Pharmacists), the provincial privacy commissioners, the Office of the Privacy Commissioner of Canada and Health Canada.

The biggest obstacle for a new entrant is fragmentation: each province sets its own licensing, privacy and record-access rules, so a national service must design identity and consent flows that satisfy the strictest province it serves.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 Identity framework (AML rules do not apply)
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Regulator	Remit	Level	Official site
Health Canada	Drugs, controlled substances and health products	Federal	canada.ca/health-canada
Office of the Privacy Commissioner of Canada	Federal private-sector privacy law (PIPEDA)	Federal	priv.gc.ca
Ontario Ministry of Health	Ontario Health Insurance Plan (OHIP), health cards, health system policy	Provincial (Ontario)	ontario.ca
Information and Privacy Commissioner of Ontario	Oversight of Ontario's health privacy law (PHIPA), penalties	Provincial (Ontario)	ipc.on.ca
College of Physicians and Surgeons of Ontario	Licensing and conduct of physicians, including virtual care	Provincial (Ontario)	cpso.on.ca
Ontario College of Pharmacists	Licensing of pharmacists and pharmacies, virtual pharmacy care	Provincial (Ontario)	ocpinfo.com
Commission d'accès à l'information du Québec	Oversight of Québec's health information and private-sector privacy laws	Provincial (Québec)	cai.gouv.qc.ca

Every other province and territory has its own medical and pharmacy regulators and privacy oversight body, which set rules for care delivered to patients located there.

2 Licensing and authorisation

No federal or provincial licence exists for a telehealth platform as such. Authorisation attaches to the people and premises that deliver care. Under the College of Physicians and Surgeons of Ontario (CPSO) Virtual Care policy (updated June 2022), physicians treating patients located in Ontario must hold a valid CPSO certificate of registration, unless care from a physician licensed elsewhere is in the patient's best interest, for example specialty care not readily available in Ontario, care that bridges a gap within an existing relationship, or urgent care (provision 16). Ontario physicians treating patients in another jurisdiction must meet that jurisdiction's licensing rules (provision 15).

Pharmacy is location-bound. The Ontario College of Pharmacists (OCP) notes that dispensing, selling or compounding drugs must take place in an accredited pharmacy, while cognitive pharmacy services can be delivered virtually from other settings.

The software itself can also be regulated. Under Health Canada's Software as a Medical Device (SaMD): Definition and Classification guidance (effective 18 December 2019), software whose intended use is a medical purpose within the definition of "device" in the Food and Drugs Act is a medical device, classified under the Medical Devices Regulations into four risk classes (Class I lowest, Class IV highest) that determine what Health Canada requires before it can be sold. Tools that only help patients organise and track their own health information are treated differently from software that diagnoses or guides treatment.

The platform operator's legal role matters as much as any licence. In Ontario, a business that supplies electronic services enabling a health information custodian to use personal health information, without being the custodian's agent, may not use or disclose that information except to provide the services; a provider serving two or more custodians as a network must also notify custodians of unauthorised access, publish a description of its safeguards and keep access logs (O. Reg. 329/04, s. 6). In Québec, a private business that agrees to provide health services on behalf of a public health body becomes a "health and social services body" for those activities under the Act respecting health and social services information (s. 4).

Identity framework (AML rules do not apply)

The PCMLTFA lists the persons and entities subject to customer identification and reporting duties in section 5: banks, credit unions, life insurers, securities dealers, money services businesses and others. Health care providers, clinics, pharmacies and health apps are not on that list, so there is no customer identification programme, suspicious transaction reporting or prescribed identity document list for the sector. A health business that also takes payments, issues stored value or offers financing should check those activities separately.

Identity duties in healthcare come instead from four sources:

Privacy statutes

An Ontario custodian must take reasonable steps to be satisfied of a patient's identity before giving access to records (PHIPA s. 54(9)). In Québec, a person requesting access to health information must prove identity and capacity (R-22.1 s. 32), as must a requester under the private-sector Act (P-39.1 s. 30).

College policies

Physicians and pharmacists must identify patients in virtual encounters (CPSO Virtual Care; OCP Virtual Care Policy v1.10). These are professional standards enforced through discipline.

Health number rules

Ontario restricts who may collect, use or demand a health number or health card (PHIPA s. 34).

Controlled substances

Pharmacists must verify the prescriber's name and signature when the prescriber is not known to them (Controlled Substances Regulations, s. 103).

Identity verification and onboarding

No Canadian health rule prescribes accepted documents, document-versus-database methods or an assurance level for private telehealth onboarding. The standard is reasonableness, scaled to the sensitivity of the encounter and whether the patient is new. The CPSO gives verifying name and date of birth as an example and notes that what is reasonable differs between an existing relationship and a new patient. OCP guidance (October 2025) suggests confirming demographic details or profile information such as previous prescriptions for existing patients, and stresses confirming the identity of anyone

acting for the patient, such as a caregiver or substitute decision-maker, so that information is not disclosed to the wrong person.

Public enrolment sets a much higher bar. Registration for OHIP is in person at ServiceOntario, with three separate original documents proving citizenship or eligible status, Ontario residency and identity. A health card is non-transferable and must be presented on request to the hospital, physician or facility providing insured services (Health Insurance Act, s. 11.1). Outside that context, no person may require production of another person's health card (PHIPA s. 34(4)).

Since 1 January 2026, Ontario Health issues "digital health identifiers", created through validation and verification services that confirm an individual's identity, with the individual's express consent (PHIPA Part V.2). The identifier gives patients digital access to drug records held in the provincial electronic health record. It is a public service, not a credential that private platforms can rely on.

Where a platform uses document capture with face matching, the biometric template is sensitive personal information (see section 6). Figure 1 shows a typical remote patient onboarding flow for virtual care in Ontario.

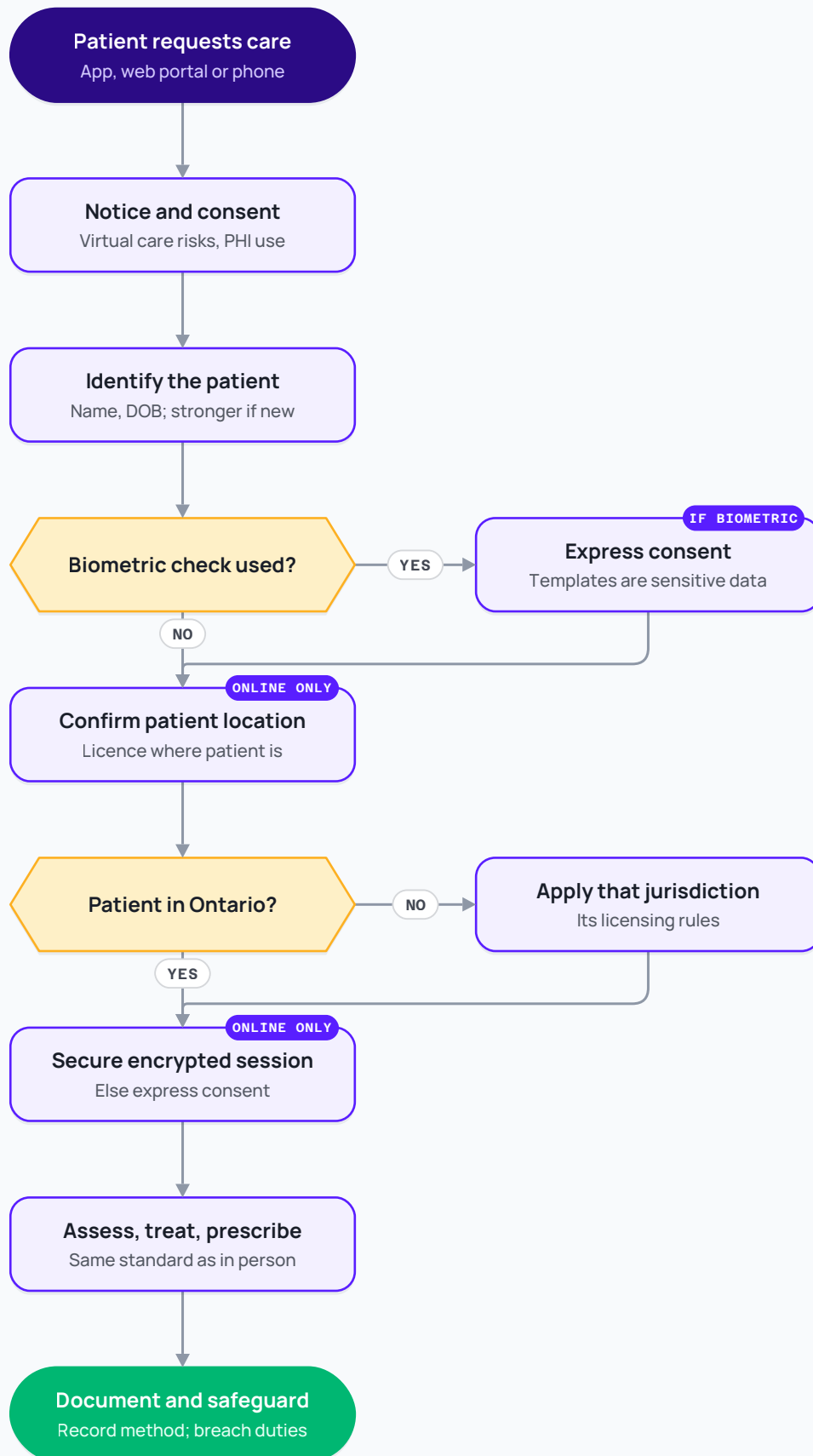


Figure 1. Remote patient onboarding for virtual care delivered to patients in Ontario.

Bottom line: privacy and prescribing rules are largely channel-neutral, but professional college policies add online-only duties: identify the patient in every virtual encounter, confirm where the patient is, use secure technology and obtain consent to the virtual modality itself.

Requirement	In person	Online / remote	Difference
Whether care may be given	Standard of care applies	Only where virtual care is in the patient's best interest	Differs
Patient identification (physicians)	Reasonable steps under general duties	Reasonable steps in each virtual encounter, e.g. name and date of birth	Differs
Patient identification (pharmacists)	Professional standards	Confirm identity and location every time, even existing patients	Differs
Patient location and licensing	Patient on premises	Licence where the patient is located, with limited exceptions	Differs
Technology and consent	Not applicable	Encrypted platform, or documented express consent to less secure tools; informed consent to the virtual modality	Differs
Identity check before giving records	Reasonable steps	Reasonable steps	Same
Demanding a health card (Ontario)	Only for publicly funded services	Only for publicly funded services	Same
Controlled substance prescriptions	Written or verbal	Written or verbal	Same
Breach notification	Required	Required	Same

Identity at every encounter, not only at onboarding

The CPSO requires physicians providing virtual care to take reasonable steps to accurately identify the patient, conduct the encounter in a private setting, disclose everyone present and ask whether the patient can speak privately (provision 11). The OCP Virtual Care Policy (version 1.10, effective 30 September 2025) goes further: pharmacists must confirm the patient's identity and location even where a relationship already exists, and the technology must have controls so that only the intended patient can join the visit. A one-time onboarding check is therefore not enough; platforms need a repeatable step at the start of each session.

Location is a licensing control

Because licensing follows the patient's physical location, the location confirmation is a compliance control, not a convenience. The OCP links it to its cross-jurisdictional pharmacy services policy for patients outside Ontario.

Secure technology and modality consent

Physicians must use secure, encrypted platforms unless the patient's best interest requires otherwise, and must obtain and document express consent before using less secure tools (provisions 11 and 12). Informed consent to the virtual modality is required at the first encounter and whenever the risks change (provisions 13 and 14). The CPSO treats the telephone as secure technology.

6 Data protection and biometrics

Which privacy law applies depends on who holds the data and where. Ontario health information custodians are governed by [PHIPA](#) and are exempt from the federal [PIPEDA](#) for activity within Ontario (SOR/2005-399). In Québec, health information held by a health and social services body falls under the Act respecting health and social services information (CQLR c. R-22.1) rather than the private-sector Act (CQLR c. P-39.1, s. 3). Private businesses in British Columbia fall under the Personal Information Protection Act. Health apps that are not custodians and operate commercially are generally under PIPEDA or the applicable provincial private-sector law.

Biometric data used to verify identity is sensitive. The Office of the Privacy Commissioner of Canada's Guidance for processing biometrics, for businesses (11 August 2025) states that biometric information capable of uniquely identifying a person is sensitive in every context and that express consent is, as a general rule, the appropriate form of consent, including for templates; it also asks organisations to show that biometrics are necessary

and proportionate. Québec's private-sector Act defines biometric information as sensitive and requires express consent for its use and communication (P-39.1 ss. 12 and 13), and requires that people be told in advance when technology can identify, locate or profile them (s. 8.1). Québec adds a specific rule for biometric identity checks: identity may be verified or confirmed with biometric characteristics only with the person's express consent and after the process has been disclosed to the Commission d'accès à l'information; only the minimum characteristics needed may be used, and the record must be destroyed once verification is complete. A biometric database must be disclosed to the Commission at least 60 days before it is brought into service (Act to establish a legal framework for information technology, CQLR c. C-1.1, ss. 44 and 45). Québec also requires a privacy impact assessment for any new information system that handles personal information (s. 3.3; for health bodies, R-22.1 s. 106) and the highest privacy settings by default (P-39.1 s. 9.1; R-22.1 s. 104).

Ontario allows a custodian to collect and use a health number with the patient's consent to identify records accurately or verify identity, even outside publicly funded services (PHIPA s. 34(6)), but a non-custodian may not collect or use another person's health number except in listed cases (s. 34(2)).

7

Sector-specific obligations

Prescribing and controlled substances

The federal Controlled Substances Regulations (SOR/2025-242) came into force on 1 October 2026, consolidating the Narcotic Control Regulations, the Benzodiazepines and Other Targeted Substances Regulations and Parts G and J of the Food and Drug Regulations. A practitioner may issue a signed and dated written prescription or a verbal prescription for a patient they are treating (s. 127). Pharmacists must verify the name, title and signature of a person sending an order or prescription if not known to them (s. 103). Health Canada's pandemic-era class exemption allowing verbal prescriptions and pharmacist extensions expired on 30 September 2026 and is replaced by the regulations.

Patient portals and record access

Ontario patients can obtain their records in an electronic format specified by Ontario Health, a PDF or another agreed format, which may include a secure portal (O. Reg. 329/04, s. 18.0.1). Any portal must apply the identity check in PHIPA s. 54(9) before release. Québec patients have the right to know who accessed their information and when (R-22.1 s. 18).

Health apps and consumer services

PHIPA s. 54.1 regulates "consumer electronic service providers" that let individuals manage their own health records, but it comes into force only on a day to be named by proclamation. Until then, consumer health apps outside the custodian relationship are governed by general private-sector privacy law.

8 Risk indicators and red flags

IDENTITY AND PRIVACY ABUSE IN DIGITAL HEALTH

- **Insider snooping for profit:** staff with record access searching patients to market private services.
- **Wrong patient in the session:** someone other than the intended patient joins or answers a virtual visit.
- **Unverified proxy:** a caller claiming to be a caregiver or substitute decision-maker without confirmation.
- **Unknown prescriber:** an order or prescription whose prescriber name or signature is not known to the pharmacist.
- **Borrowed health card:** a card presented by someone other than the insured person, although cards are non-transferable.
- **Out-of-province patient:** a patient located outside the clinician's licensing jurisdiction.
- **Re-identification:** attempts to identify individuals from de-identified health data, prohibited by PHIPA s. 11.2.

9 Enforcement and penalties

Regime	Penalty basis	Maximum
PHIPA administrative penalties (Ontario)	Per order, for any number of contraventions, set by criteria such as harm, number affected and economic benefit	\$50,000 individual; \$500,000 organisation, plus any economic benefit (O. Reg. 329/04, s. 35)

PHIPA offences (Ontario)	On conviction; officers who authorise an offence are also liable	\$200,000 and up to 1 year for individuals; \$1,000,000 for organisations (s. 72)
PIPEDA offences (federal)	Knowingly failing to report breaches or keep breach records, obstruction	\$10,000 summary; \$100,000 indictable (s. 28)
Québec administrative penalties	Per failure, under a published framework	\$50,000 individual; otherwise \$10,000,000 or 2% of worldwide turnover (P-39.1 s. 90.12)
Québec penal offences	Per offence; doubled for repeat offences	\$100,000 individual; otherwise \$25,000,000 or 4% of worldwide turnover (P-39.1 ss. 91, 92.1)

In PHIPA Decision 298 (2025), the Information and Privacy Commissioner of Ontario issued the first administrative penalties under PHIPA. A physician had used his access to several hospitals' shared electronic health record to search for newborn boys and offer their parents services at his private clinic. The Commissioner imposed \$5,000 on the physician and \$7,500 on the clinic, ordered secure disposal of the records obtained, and stressed that custodians must have a privacy management programme in place before opening for business.

10 Recent changes and what to watch

- **1 October 2026:** Controlled Substances Regulations in force **In force**. Verbal prescribing and pharmacist prescription transfers now rest on the regulations rather than a temporary exemption.
- **15 June 2026:** Bill C-36, the proposed Protecting Privacy and Consumer Data Act, introduced **Bill, not enacted**. It would replace Part 1 of PIPEDA, expressly treat health information and biometric information capable of uniquely identifying a person as sensitive, require security safeguards to include reasonable measures to authenticate the identity of the individual, and allow penalties up to the greater of \$10,000,000 and 3% of gross global revenue (ss. 2, 56(3) and 114). It was at second reading in the House of Commons as of 27 October 2026, so PIPEDA continues to apply.
- **1 January 2026:** Ontario's digital health identifier regime (PHIPA Part V.2) in force **In force**. Ontario Health verifies identity, with express consent, to give patients digital access to drug records.

- **1 January 2027 and 2028:** lab records added to digital access, then an alternative access process for people who cannot or do not wish to use the digital route
Adopted, effective 1 Jan 2027 and 1 Jan 2028.
- **30 September 2025:** OCP Virtual Care Policy version 1.10 effective **In force**, with supplemental guidance in October 2025 on confirming identity and location.
- **11 August 2025:** OPC biometrics guidance for businesses adopted **In force**. Expect express consent and proportionality to be tested in investigations.
- **Date to be named:** PHIPA electronic audit log duty (s. 10.1) and consumer electronic service provider rules (s. 54.1) *Adopted, effective date not yet set*. Québec's access-logging duty for health bodies (R-22.1 s. 103) is likewise not yet in force.

11 What this means for identity verification

Design for "reasonable steps", documented. Because no rule prescribes a method, the record of what was checked and why becomes the evidence of compliance. Use a stronger check for new patients and for higher-risk actions such as releasing records or prescribing, and a lighter confirmation for returning patients.

Build a per-session step. Ontario pharmacists must confirm identity and location at every virtual interaction, and physicians must identify the patient in each encounter. Session-level re-confirmation, such as a returning-user face match or knowledge check combined with a location prompt, maps directly to these duties.

Avoid health cards as general ID. Use government photo identity documents for document-based checks, and collect health numbers only when providing publicly funded services or where PHIPA s. 34 permits.

Treat biometrics as sensitive: obtain express consent, explain alternatives and limit template retention. Verify proxies and substitute decision-makers as carefully as patients. Expect regional variation, and keep identity and consent evidence available for breach investigations and access requests.

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Remote patient onboarding with ID document capture and verification, including NFC chip reading of passports.
- Face match and biometric liveness for returning-patient checks at the start of each virtual session, with consent capture.
- Phone and email verification for patient accounts and for caregivers or substitute decision-makers acting for a patient.
- A no-code workflow builder to apply stronger checks for new patients, record access and prescribing, with an audit trail for each check.
- Cloud, on-premises or hybrid deployment to keep health data where provincial rules and internal policies require.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A** (consolidation from 1 January 2026; ss. 10.1, 11.2, 12, 34, 54(9), 54.1, Part V.2, 61.1, 72), Ontario e-Laws, [ontario.ca/laws/statute/04p03](https://e-laws.gov.on.ca/laws/statute/04p03)
- **O. Reg. 329/04, General** (consolidation from 1 January 2026; ss. 6, 6.3, 6.4, 18.0.1, 18.1, 18.1.1, 18.16, 35), Ontario e-Laws, [ontario.ca/laws/regulation/040329](https://e-laws.gov.on.ca/laws/regulation/040329)
- **Health Insurance Act, R.S.O. 1990, c. H.6, s. 11.1**, Ontario e-Laws, [ontario.ca/laws/statute/90h06](https://e-laws.gov.on.ca/laws/statute/90h06)
- **Apply for OHIP and get a health card** (updated 21 July 2025), Government of Ontario, ontario.ca

- **Virtual Care policy** (reviewed and updated June 2022), College of Physicians and Surgeons of Ontario, cpso.on.ca
- **Virtual Care Policy, version 1.10** (approved 16 September 2025, effective 30 September 2025), Ontario College of Pharmacists, ocpinfo.com
- **Supplemental Guidance to the Virtual Care Policy** (15 October 2025), Ontario College of Pharmacists, ocpinfo.com
- **Controlled Substances Regulations, SOR/2025-242** (ss. 103, 127, 239), Justice Laws Website, laws-lois.justice.gc.ca; Regulatory Impact Analysis Statement, Canada Gazette, Part II, 17 December 2025, gazette.gc.ca
- **Subsection 56(1) class exemption for patients, practitioners and pharmacists prescribing and providing controlled substances in Canada** (page modified 17 December 2025), Health Canada, canada.ca
- **Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17, s. 5**, Justice Laws Website, laws-lois.justice.gc.ca
- **Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, ss. 4, 10.1, 28**, Justice Laws Website, laws-lois.justice.gc.ca
- **Health Information Custodians in the Province of Ontario Exemption Order, SOR/2005-399**, Justice Laws Website, laws-lois.justice.gc.ca
- **Guidance for processing biometrics, for businesses** (11 August 2025), Office of the Privacy Commissioner of Canada, priv.gc.ca
- **Bill C-36, An Act to enact the Protecting Privacy and Consumer Data Act**, 45th Parliament, 1st session, LEGISinfo, parl.ca; first reading text, parl.ca
- **Loi sur les renseignements de santé et de services sociaux [Act respecting health and social services information]**, CQLR c. R-22.1 (updated to 15 October 2026; ss. 4, 18, 32, 103 to 108), LégisQuébec, legisquebec.gouv.qc.ca
- **Loi sur la protection des renseignements personnels dans le secteur privé [Act respecting the protection of personal information in the private sector]**, CQLR c. P-39.1 (updated to 15 October 2026; ss. 3, 3.3, 8.1, 9.1, 12, 13, 30, 90.12, 91, 92.1), LégisQuébec, legisquebec.gouv.qc.ca
- **Loi concernant le cadre juridique des technologies de l'information [Act to establish a legal framework for information technology]**, CQLR c. C-1.1, ss. 44 and 45, LégisQuébec, legisquebec.gouv.qc.ca
- **Guidance Document: Software as a Medical Device (SaMD): Definition and Classification** (effective 18 December 2019), Health Canada, canada.ca
- **Personal Information Protection Act, SBC 2003, c. 63** (current to 20 October 2026), BC Laws, bclaws.gov.bc.ca
- **First administrative monetary penalty issued under Ontario's health privacy law**, Information and Privacy Commissioner of Ontario, ipc.on.ca; PHIPA Decision 298 summary, IPC latest decisions, ipc.on.ca