Practice Guideline

Information Privacy and Management Legislation

Prepared August 2020
Updated December 2025

Guideline Contents

1. Introduction 2
2. Provincial Legislation 3
   Health Information Act (HIA) 3
   Protection of Privacy Act (POPA) and the Access to Information Act (ATIA) 4
   Personal Information Protection Act (PIPA) 6
   Children First Act (CFA) 6
3. Federal Legislation 8
   Privacy Act 8
   Personal Information Protection and Electronic Documents Act (PIPEDA) 8
4. Employer or Contracting Organization Policy and Procedure 9
5. Consent Considerations 10
6. Access to Information and Requests for Corrections 11
7. Information Storage and Record Retention Considerations 12
8. Reporting Privacy Breaches 14
9. References and Additional Resources 15

Appendix A – Relevant Clauses and Indicators in ACOT's *Standards of Practice* and *Code of Ethics* and the *Competencies for Occupational Therapists in Canada* 16

Appendix B – Which Privacy Legislation Applies 20

Appendix C – Information Access and Disclosure Processes 21

Contact ACOT at info@acot.ca or 780.436.8381 with questions about this guideline.

Definitions of **bolded** terms found in this document are available in the glossaries of ACOT's *Standards of Practice* and *Code of Ethics*.

1. Introduction

This practice guideline supports **registrants** of the Alberta College of Occupational Therapists (ACOT) to gain awareness and understanding of the information privacy and management legislation that may apply to their practice. It outlines expectations for the appropriate and ethical collection, use, access, disclosure and retention of information (i.e., information management). The guideline builds on the privacy, confidentiality, communication, documentation and record retention, and risk management requirements and competencies set out in ACOT's *Standards of Practice* (SoP), *Code of Ethics* (CoE) and the *Competencies for Occupational Therapists in Canada* (see Appendix A for relevant clauses).

Various provincial and federal Acts govern information privacy and management in Alberta. Registrants are expected to be knowledgeable of and practice in accordance with legislation relevant to their practice situation (SoP A.2). The legislation that applies in each practice situation depends on several factors, including:

- The registrant's employer or contracting organization (e.g., public, private, federal government)
- The **client** population served (e.g., children or adults)
- Type of information (e.g., personal or health information)
- Location of the client at the time of service delivery (e.g., remote, different jurisdiction from the registrant)
- A need for cross provincial/territorial border information sharing

In some practice situations, more than one legislative Act may apply (See Appendix B).

While the specific requirements vary by Act, the following core principles are consistent across provincial and federal privacy and information management legislation:

- Collect, use and disclose only the minimum personal and health information required for the intended purpose

- Obtain **consent** before collecting, accessing or disclosing client information unless the legislation applicable to the specific practice **context** explicitly allows otherwise

Some specific considerations related to consent to collect, use and disclose information are elaborated on in this guideline. For the full list of consent requirements under each Act, please refer to the relevant legislation (see also References and Additional Resources). For guidance related to information sharing in the context of required reporting (e.g., suspected abuse), please see ACOT's *Duty to Report* practice guideline.

2. Provincial Legislation

This section describes relevant Alberta legislation and identifies practice situation(s) that may apply.

- *Health Information Act* (HIA)
- *Protection of Privacy Act* (POPA)
- *Access to Information Act* (ATIA)
- *Personal Information Protection Act* (PIPA)
- *Children's First Act* (CFA)

Health Information Act (HIA)

The *Health Information Act* (HIA) governs the collection, use and disclosure of health information by "custodians" and their "affiliates". Health information includes (1) registration information (such as name, personal health number, gender, date of birth) and (2) diagnostic, treatment and care information. Custodians and affiliates are defined in HIA and the *Health Information Regulation* (HIR) and include:

Custodians:

- Provincial health agencies (Acute Care Alberta, Assisted Living Alberta, Primary Care Alberta, Recovery Alberta)
- Provincial health corporations and contracted health service providers (e.g., Alberta Health Services (AHS), Covenant Health, Lamont Health Care Centre, Cancer Care Alberta, Emergency Medical Services)
- Continuing care homes as defined in the *Continuing Care Act*
- Regulated chiropractors, optometrists, pharmacists, dentists, registered nurses, denturists, midwives, opticians, physicians and surgeons, podiatrists and dental hygienists

Affiliates:

- Any employee of a custodian
- A person that performs a service for a custodian such as a volunteer or student or person under a contract with the custodian
- A custodian that wishes to be an affiliate of another custodian for the ease of information sharing

See the HIA and HIR for the complete definitions and listing of custodians and affiliates.

When does the HIA Apply?

Occupational therapists are not considered to be custodians under the HIA or HIR. However, the HIA governs health information collected in connection with the provision of a health service by an occupational therapist (OT) if/when the OT is employed or contracted by a custodian or affiliate. Many ACOT registrants work in positions where they are affiliates in relation to the health information they collect during service provision. Whether the OT works for or is contracted by a custodian or an affiliate, the OT is required to follow and adhere to HIA and the information privacy and management policies and procedures set out by the custodian/affiliate by whom they are employed or contracted.

NOTE: *Registrants in private practice must adhere to the requirements outlined in the Personal Information and Privacy Act (PIPA). They do not have obligations under HIA unless they are contracted by a custodian or affiliate as defined in HIA or they are providing services under the Diagnostic and Treatment Protocols Regulation (DTPR). HIA applies to DTPR records.*

Protection of Privacy Act (POPA) and the Access to Information Act (ATIA)

The *Protection of Privacy Act* (POPA) and the *Access to Information Act* (ATIA) replaced the former *Freedom of Information and Protection of Privacy Act* (FOIP) in 2025.

POPA governs the collection, use and disclosure of personal information by "public bodies". Personal information is defined in POPA and includes identifiable information about a person such as their name; age; gender; address; contact information; health and health care history; educational, financial, employment or criminal history; or an individual's personal views or opinions (unless they are about another individual).

ATIA supports public accountability through a right of access to records under the control of public bodies, subject to limited and specific exceptions described in the Act. ATIA outlines the rules and processes for accessing records, including accessing one's own information held by public bodies (including the Alberta Government).

A public body is defined for both these acts in ATIA as:

- Alberta government department, branch or office
- Agency, board, commission, corporation, office or other body designated as a public body by the Designation of Public Bodies Regulation (e.g. *Workers' Compensation Board* - WCB[1])
- Local public bodies (e.g. school boards, health care bodies such as hospitals, universities/colleges/technical institutes, municipality or a municipal board)

The POPA and ATIA apply to all records in the public body's custody or control. Records are broadly defined to include information in any form (e.g., written, electronic, digital, photographic, audio, etc.), and can include information contained or stored in any manner. Health information held by a public body has additional requirements and restrictions under the *Health Information Act*.

When do the POPA and ATIA apply?

Both the POPA and ATIA apply to registrants who are employees, contractors or volunteers of a public body. This includes registrants employed or contracted by an early childhood services (ECS) provider; school board, school or school district; any organization that receives funding from Alberta Education, Children and Family Services, or Seniors, Community and Social Services; or other public or local public bodies defined in POPA.

POPA and ATIA also apply when registrants are employed or contracted by a HIA custodian but regarding information that is not health information (e.g., employment records). ATIA applies specifically to situations where an individual requests access to records held by a public body, including personal information about themselves.

[1] Occupational therapists or employers with WCB contracts are also governed by the *Workers' Compensation Act*, which gives the WCB a right of access to information in a patient's file. POPA may also apply to records related to WCB claims depending on the circumstances.

Personal Information Protection Act (PIPA)

The *Personal Information Protection Act* (PIPA) governs the collection, use and disclosure of personal information for reasonable purposes by private sector organizations, businesses, professional regulatory organizations and some non-profit organizations.

When does the PIPA Apply?

PIPA applies to the personal, employee or client information collected, used and disclosed by registrants in private practice (e.g., sole proprietor or group/clinic). Registrants who are contracted by an organization in the private sector should seek to have the responsibilities for information privacy, disclosure, access and retention clearly outlined in the terms of their contract. Self-employed registrants are expected to establish policies and procedures aligned to applicable legislation (SoP A.5) including information privacy and management.

Children First Act (CFA)

The *Children First Act* (CFA) enhances existing legislation, processes and policies to support the health, safety, education, security and well-being of children. The CFA guides appropriate information sharing between individuals and organizations that plan or provide programs and services for children.[2] In addition to current information sharing provisions found in the HIA and POPA, the CFA outlines additional circumstances where information can be shared, if necessary, without consent, but only when in the best interests of the child.

The CFA authorizes the collection, use and disclosure of health information or personal information *without consent* in the circumstances and for the purposes described in sections 4 (provision of services) and 5 (research) of the CFA. Disclosure without consent is only permitted under section 4 of the CFA if:

- The disclosure is for the purpose of enabling or planning for the provision of services or benefits to a child (s. 4(2));
- The disclosure is in the best interests of the child (ss. 4(2), 4(3));
- With respect to disclosure to the child's guardian, the child has not expressly requested that the disclosure not be made (s. 4(3)); and,

[2] Source: guide-to-information-sharing-under-the-children-first-act.pdf (SECURED)

- The CFA applies to the practice setting (see below).

While the CFA authorizes disclosure without consent in certain circumstances, the CFA does not preclude health care providers from seeking and obtaining consent. Requesting consent before sharing information demonstrates respect for client autonomy. If sharing information without consent, ensure to document the rationale for doing so, addressing why this aligns with the child's best interest.

When does the CFA Apply?

The CFA applies to HIA custodians and affiliates as well as "service providers". Service providers are defined in the CFA and include:

- Educational bodies (as defined in the POPA)
- An individual or organization that provides programs or services for children under an agreement with a "public body" (as defined in the POPA)
- Government departments (as defined in the *Government Organization Act*)
- Police Services (as defined in the *Police Act*)

This means that the CFA applies to registrants employed or contracted by custodians and affiliates (as defined in the HIA) and educational bodies and public bodies (as defined in the POPA). This includes registrants employed or contracted with school boards, schools or agencies/organizations that receive funding from Alberta Education or Children's Services (e.g. early childhood service providers). It also applies to registrants delivering services under Family Supports for Children with Disabilities (FSCD).

The CFA *does not* apply to registrants who are working in the private sector *and* who do not complete work for custodians, affiliates or public bodies. These private practice registrants must adhere to the rules set out in PIPA for when information can be collected, used or disclosed without consent when planning and providing services to children.

Please refer directly to the CFA, HIA, POPA, PIPA and the Alberta Government's *Guide to Information Sharing under the Children First Act* for further guidance when applying the CFA to a specific practice context.

3. Federal Legislation

This section describes relevant federal legislation and identifies practice situation(s) that may apply.

- *Privacy Act*
- *Personal Information Protection and Electronic Documents Act* (PIPEDA)

Privacy Act

The *Privacy Act* governs the collection, use and disclosure of personal information by or for federal government institutions. Personal information under the *Privacy Act* means information about an identifiable individual that is recorded in any form. The types of information included in this definition are outlined in section 3 of the Act.

When does the Privacy Act Apply?

This Act applies to registrants working for a Government of Canada institution or submitting or handling information to/for:

- Veteran's Affairs
- Indigenous Services Canada (e.g., Non-Insured Health Benefits, Jordon's Principle, Inuit Child First Initiative, etc.)
- Canada Revenue Agency (e.g., Disability Tax Credit)
- Other federal government institutions.

Personal Information Protection and Electronic Documents Act (PIPEDA)

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is federal legislation that establishes the rules for the collection, use, disclosure of and access to personal information for private sector organizations conducting commercial activities[3]. Under the PIPEDA, personal information includes any factual or subjective information, recorded or not, about an identifiable individual[4].

[3] See also Interpretation Bulletin: Commercial Activity - Office of the Privacy Commissioner of Canada
[4] See also PIPEDA requirements in brief - Office of the Privacy Commissioner of Canada

When does the PIPEDA Apply?

Alberta has their own private-sector privacy law, the PIPA, which has been deemed "substantially similar to" the PIPEDA. Organizations subject to a substantially similar provincial privacy law are generally exempt from the PIPEDA with respect to the collection, use or disclosure of personal information that occurs within that province[5]. In other words, registrants will typically follow the requirements of PIPA.

However, it is possible in some situations that both PIPA and the PIPEDA will apply, and therefore both Acts must be complied with. One example is cross border information sharing. The PIPEDA applies to registrants where client information is being transferred across provincial or territorial boundaries in Canada. This includes communicating and/or delivering **occupational therapy services** to clients who are physically located in a different province or territory or communicating with a third-party insurer or funder in another province or territory.

For registrants working with First Nations organizations, note that the PIPEDA also applies to First Nations Band and Tribal councils[6] engaged in commercial activities.

4. Employer or Contracting Organization Policy and Procedure

Along with ensuring adherence to applicable provincial and federal legislation, registrants must follow their employer or contracting organization's policies and procedures related to privacy and information management. This includes policies and procedures developed and adopted by First Nations, Inuit and Metis organizations. An employer or organization's policies and procedures must not prevent registrants from meeting the minimum expectations of ACOT's Standards of Practice and Code of Ethics (SoP A.4, A.5). Where employer or contracting organization policies are more stringent, the registrant should follow the employer or organization's direction.

Appendix C provides a summary diagram outlining privacy and access processes under Alberta and federal legislation. This diagram may be helpful as a summary resource when used in conjunction with employer or contracting organizations' policies and procedures.

[5] Provincial laws that may apply instead of PIPEDA - Office of the Privacy Commissioner of Canada
[6] A First Nations Guide to the Personal Information and Electronic Documents Act (PIPEDA) The First Nations Information Governance Centre (2023)

5. Consent Considerations

As outlined in the Introduction of this guideline, consent is required from the individual prior to collecting, using or disclosing their personal or health information. However, there are additional considerations or exceptions depending on the applicable legislation. Some notable considerations specific to HIA, PIPA and CFA are:

HIA

Consent from a client or **substitute decision maker** is not required before a custodian or affiliate can disclose health information to another custodian or affiliate for the purpose of continuity of care or client safety. More information: Health Information Act | Alberta.ca

PIPA

There are limited situations outlined in PIPA where collection, use or disclosure of personal information may occur without consent, including when it is legally authorized by another statute/legislation of Alberta or Canada. See Collecting personal information | Alberta.ca and PIPA Section 20 for a full listing of situations when consent is not required.

CFA

Personal information relating to a child or their substitute decision maker, or health information relating to a child may be released without consent if the disclosure is in the child's best interest or for safety concerns (e.g., suspected child abuse, neglect and exploitation under the *Child Youth and Family Enhancement Act*). If the child has expressly requested information not be disclosed to their guardian, the information cannot be disclosed under the authority of the CFA. However, if disclosure is necessary to avert or minimize the risk of harm to the health or safety of a child younger than 18, the person disclosing must consider whether disclosure is permitted by the HIA or POPA harm provisions. More information on to whom, when and for what purpose a child's personal and health information can be released can be found in the CFA and the related Guide to Information Sharing under the *Children First Act*.

6. Access to Information and Requests for Corrections

Individuals have the right to access and request corrections to their personal or health information held by public bodies, private organizations and businesses, or federal institutions. Requests are typically made in writing to the designated privacy coordinator/officer within the organization/institution. Organizations usually have a legislated timeline (e.g., 30 days) they must respond within or provide a reason for refusal. Access may be refused in limited circumstances such as regarding information collected for a legal proceeding, confidential commercial information, or information that could reasonably threaten someone's safety or reveal another person's personal information or confidential identity.

Refer to the Act(s) related to the practice context, for the specific access and correction/amendment requirements. For more information see the following links.

HIA:

- Health Information Act | Alberta.ca.
- Request to Access Health Information Form

ATIA:

- Access to information requests | Alberta.ca

PIPA:

- Accessing your personal information | Alberta.ca

The Privacy Act:

- Accessing your personal information – federal government - Office of the Privacy Commissioner of Canada.

PIPEDA:

- Accessing your personal information – businesses - Office of the Privacy Commissioner of Canada

7. Information Storage and Record Retention Considerations

Registrants must maintain accurate, complete, legible and **timely** client records that are stored, retained and shared in compliance with legislation and ACOT requirements (SoP E. Documentation and Record Retention). Clients should expect that their occupational therapy service records are accurate, complete and protected from unintended disclosure.

ACOT SoP E.8 requires registrants to retain client records for at least 11 years and 3 months after the last date of service or in the case of a minor, for at least eleven years and three months after the client turns eighteen years of age. Due to variations in the expectations set in legislation, employers or contracting organizations may have different record retention schedules. If employer/organization policies differ from ACOT standards, registrants must first address the discrepancy with the employer (SoP A.4 and E.5). If the issue cannot be resolved, preventing the registrant from meeting ACOT minimum standards, the registrant should contact ACOT.

HIA

Under the HIA section 60, custodian/affiliates must protect the confidentiality and security of health information throughout the entire record lifecycle. HIA does not prescribe storage methods or retention timelines, leaving this to the custodian's discretion to set storage and retention policies.

POPA

Public bodies must protect personal information from unauthorized access, use, disclosure or destruction and they must establish a privacy management program. Public bodies must ensure that personal information is accurate, complete and retained for at least one year after use. Each public body sets its own record retention schedule. Accordingly, the employer or contracting organization should have record storage and retention policies in place that the registrant can refer to.

PIPA

Under PIPA section 35, personal information may be retained only as long as necessary for legal or business purposes. An example of a "legal purpose" to retain records would be if a client or their substitute decision maker disagrees with the results or recommendations of an assessment and decides to file a civil lawsuit.

In Alberta, civil actions may be filed up to 10 years after the event. This timeline is extended by up to another year and three months to serve the filed action in accordance with the *Limitations Act*. This aligns with ACOT SoP E.8 retention requirements. Client

records can be retained longer, if it is known that information will be required for a valid reason (e.g., pending legal action).

NOTE: *For registrants employed or contracted by school boards/districts, private schools or private operators of early childhood services (ECS) programs, there is additional guidance on record retention and disclosure in the Student Record Regulation including the length of time students' records are to be retained.*

CFA

The *Disclosure of Information Regulation*, requires records of disclosures made under the CFA to be established and include:

- a description of the information disclosed,
- the date of the disclosure, and
- the name of the person or entity to whom/which the information was disclosed.

While it is not explicitly written in the *Disclosure of Information Regulation*, it is prudent to also document the reason for the disclosure. The record must be maintained for 10 years after being created and then disposed of according to the service provider or custodian's records disposition policy.

The Privacy Act

Under the *Privacy Act*, personal information must be retained long enough to ensure individuals have a reasonable opportunity to access it, with retention schedules established by each federal institution.

PIPEDA

Organizations or businesses subject to the PIPEDA must protect personal information against loss, theft, or any unauthorized access, disclosure, copying, use or modification. The PIPEDA states that personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous, permitting the organization to develop record retention schedules and polices at their discretion.

8. Reporting Privacy Breaches

Registrants must identify and mitigate risks to a client's privacy and confidentiality [SoP K.3(f)]. This includes acting to prevent and report privacy breaches. A privacy breach means any loss, unauthorized access, or unauthorized disclosure of personal information or individually identifying health information [*Office of the Privacy Commissioner of Alberta (OIPC)*]. This applies to both client and employee information.

The OIPC maintains a webpage[7] that provides privacy breach reporting information, including:

- Requirements to notify the commissioner,
- Guidance for:
    - private sector organizations under PIPA
    - health custodians (and affiliates) under HIA
    - public bodies under POPA, and
- Resources on privacy breach response and notification.

Individuals working for or contracted to a federal institution must follow the Office of the Privacy Commissioner of Canada (OPC) requirements for breach reporting[8].

In addition to following the provincially and federally legislated requirements, registrants should follow the privacy breach reporting procedures of the organization they work for, which may entail reporting the breach to a designated person (e.g., privacy officer) who in turn will make the report to the OIPC or OPC.

A common rule across legislation and the public and private sectors is that a breach must be reported if there is a *real risk of significant harm* to an individual.

Breach reporting forms and resources:

- OIPC: How to Report a Privacy Breach
- OPC: Respond to privacy breaches at your federal institution - Office of the Privacy Commissioner of Canada.

[7] Breach Notification Requirements | OIPC of Alberta

[8] What you need to know about mandatory reporting of breaches of security safeguards - Office of the Privacy Commissioner of Canada

9. References and Additional Resources

College of Licensed Practical Nurses of Alberta (CLPNA)

- Privacy Legislation Flowchart
- Privacy Legislation in Alberta (2024)

College of Physiotherapists of Alberta (CPTA) – Privacy Guide for Alberta Physiotherapists. (March 2019)

First Nations Information Governance Centre – A First Nations Guide to the Personal Information and Electronic Documents Act (PIPEDA) (2023)

Government of Alberta

- Disclosing personal information
- ATIA Resources for Albertans
- POPA Resources | Alberta.ca
- Health Information Act guidelines and practices manual
- Information management and sharing education
- Organization responsibilities for protecting personal information
- Guide to information sharing under the Children First Act
- Information Sharing Under the Children First Act (free e-learning module)
- *Student Record Regulation*
- *Government Organization Act*

Government of Canada

- Privacy Guide for Businesses
- Protecting your information and data when using applications- ITSAP.40.200 - Canadian Centre for Cyber Security

Office of the Information and Privacy Commissioner of Alberta (OIPC)

- Privacy Laws in Alberta
- Guidelines for Obtaining Meaningful Consent. (Includes a checklist of considerations for informing your clients about the information you are collecting and potentially disclosing.)
- Privacy Breach Response, Reporting and Notification.

Office of the Privacy Commissioner of Canada (OPC)

- Respond to privacy breaches at your federal institution - Office of the Privacy Commissioner of Canada
- Provincial laws that may apply instead of the PIPEDA - Office of the Privacy Commissioner of Canada

Appendix A – Relevant Clauses and Indicators in ACOT's *Standards of Practice* and *Code of Ethics* and the *Competencies for Occupational Therapists in Canada*

ACOT Standards of Practice

Standard	Applicable Section(s)
A. Accountability and Professional Responsibility	*2. Is knowledgeable of and practices in accordance with legislation relevant to their practice situation and ACOT's Standards of Practice and Code of Ethics.* *3. Is responsible and accountable for the occupational therapy services provided by themselves and any person(s) they are responsible for supervising.* *4. Takes reasonable steps to ensure employer or contracting organization policies, procedures or processes do not prevent the registrant from meeting the expectations outlined in ACOT's Standards of Practice, Code of Ethics and practice guidance documents.* *5. In situations of self-employment, has processes in place for themselves and any persons they are responsible for supervising, which are consistent with legislation relevant to their practice situation and ACOT's Standards of Practice, Code of Ethics and practice guidance documents.* *10. Complies with all legal duties to report including, without limitation, any reporting requirements concerning children in need of intervention or the abuse of persons in care.*

Standard	Applicable Section(s)
C. Communication	*3. Maintains confidentiality and receives a client's **informed consent** as required prior to communicating or sharing personal and/or health information with persons other than a client.*
E. Documentation and Record Retention	*4. Maintains all documentation, correspondence and other records collected/stored in any form (e.g., paper, electronic, audio, photo, video, etc.) in compliance with applicable legislation, regulatory requirements, Standards of Practice, Code of Ethics, employer policies, and as applicable, the copyright permissions or licensing requirements of any standardized tools used.* *5. When serving as an affiliate of a custodian (as defined in the Health Information Act), the registrant ensures their requirements for record keeping are aligned with the policies and procedures of the custodian. Where the minimum standards identified in ACOT's Standards of Practice are not aligned to the custodian's requirements for record keeping, the registrant promptly reports the discrepancy to the custodian and ACOT for further consideration.* *6. Ensures that client records (either paper or electronic) incorporate an audit trail that clearly captures any alterations made to a client record including who accessed the record, who made the change or addition, and the date the change or addition was made.* *7. Backs-up electronic records to ensure access to client information in the event records are compromised.* *8. Retains client records for at least eleven (11) years and three (3) months after the last date of service or in the case of a minor, for at least eleven (11) years and three (3) months after the client turns eighteen (18) years of age* *(a) Client records can be retained beyond this time period if it is reasonably known that information will be required for a valid reason*

Standard	Applicable Section(s)
	such as notification of a pending legal proceeding. *9. Disposes of or transfers client records in a manner that maintains the security and confidentiality of client information. (a) Takes appropriate actions to prevent abandonment of client records (e.g., when retiring from, closing or transferring ownership of a private practice).* *10. Provides a copy of client records to the client upon the client's request in accordance with employer policies or contract where applicable.*
I. Privacy and Confidentiality	Full Standard, pages 39-40
K. Risk Management and Safety	*3. Identifies **risks** in practice and incorporates measures to mitigate and/or manage these risks. Risks include but are not limited to…* *(f) breaches of client privacy or confidentiality.* *4. Incorporates **risk management** approaches in service provision as appropriate for the client's priorities, needs, and circumstances, and the practice situation.*

ACOT Code of Ethics

Code	Ethical Responsibility
B. Responsibilities to Clients	*Registrants have an ethical responsibility to …* *1. Provide occupational therapy services that uphold the dignity of each client.* *3. Respect a client's choice regarding the involvement of family members and/or care partners in service planning and delivery.* *7. Communicates transparently to clients the occupational therapist's obligations and constraints of funding sources, employers, or referral sources.*
D. Responsibilities to the Public and the Profession	*Registrants have an ethical responsibility to:* *1. Maintain a level of professional conduct that does not* *(a) exploit or cause harm to others; or* *(b) diminish the public's trust in the profession.* *2. Recognize systems of inequity in their practice* ***context*** *and Act within their professional sphere of influence to address and prevent racism and other forms of discrimination or oppression.* *3. Act transparently and with integrity in all professional and business activities (e.g., fees and billing, contracts or terms of agreement with clients or contracting organizations, advertising of professional services, use of social media or other online platforms, response to any real or perceived* ***conflicts of interest****, etc.)*

Competencies for Occupational Therapists in Canada (ACOTRO, ACOTUP & CAOT, 2021/2024) (French Version)

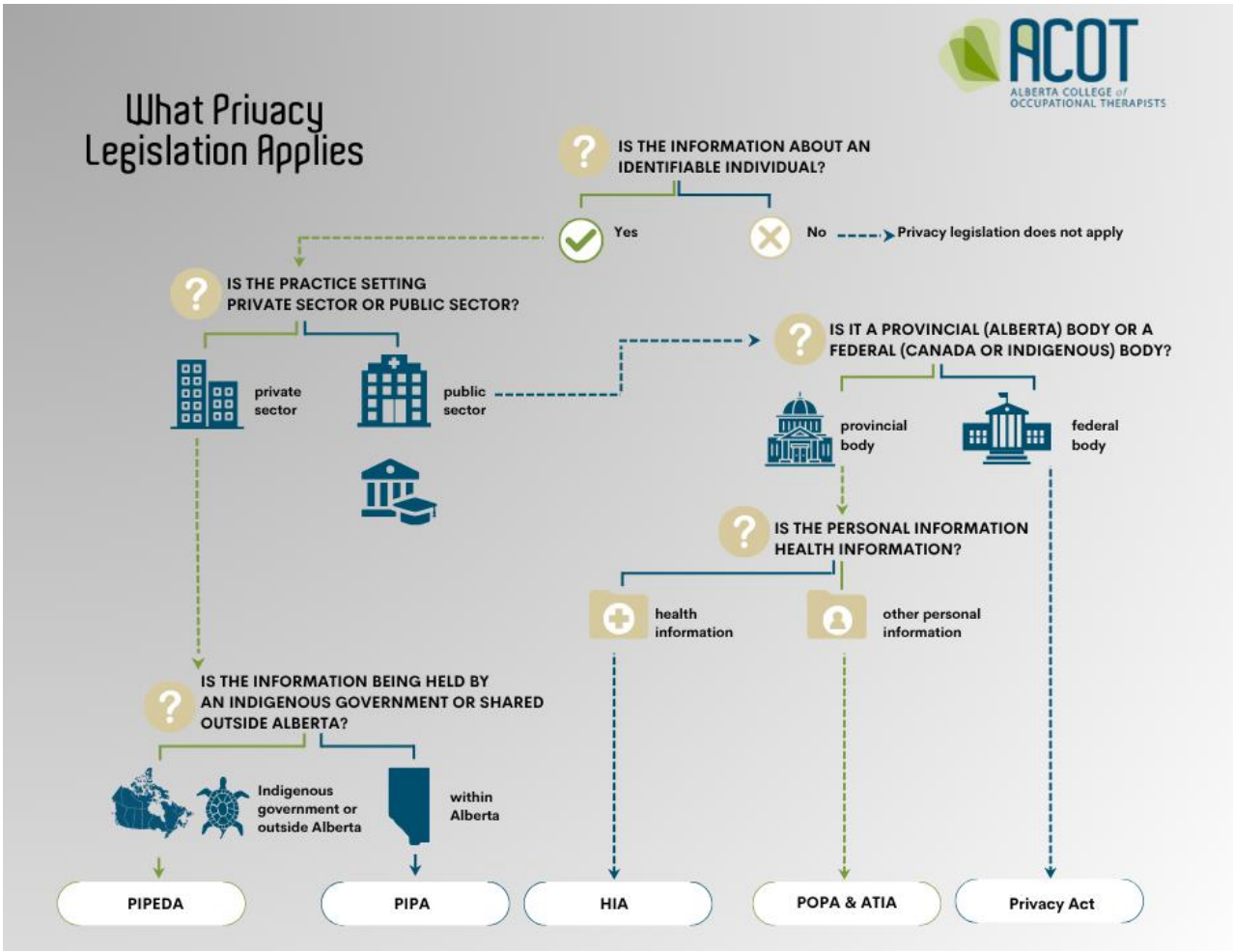
Domain B: *Communication and Collaboration* (p.12)

We listen, share, and work with others. Occupational therapy practice relates to people. Occupational therapists build respectful relationships with clients, team members, and others involved in the systems in which they work. The competent occupational therapist is expected to: …

B2.2 *Maintain confidentiality, security, and data integrity in the sharing, transmission, storage, and management of information.*

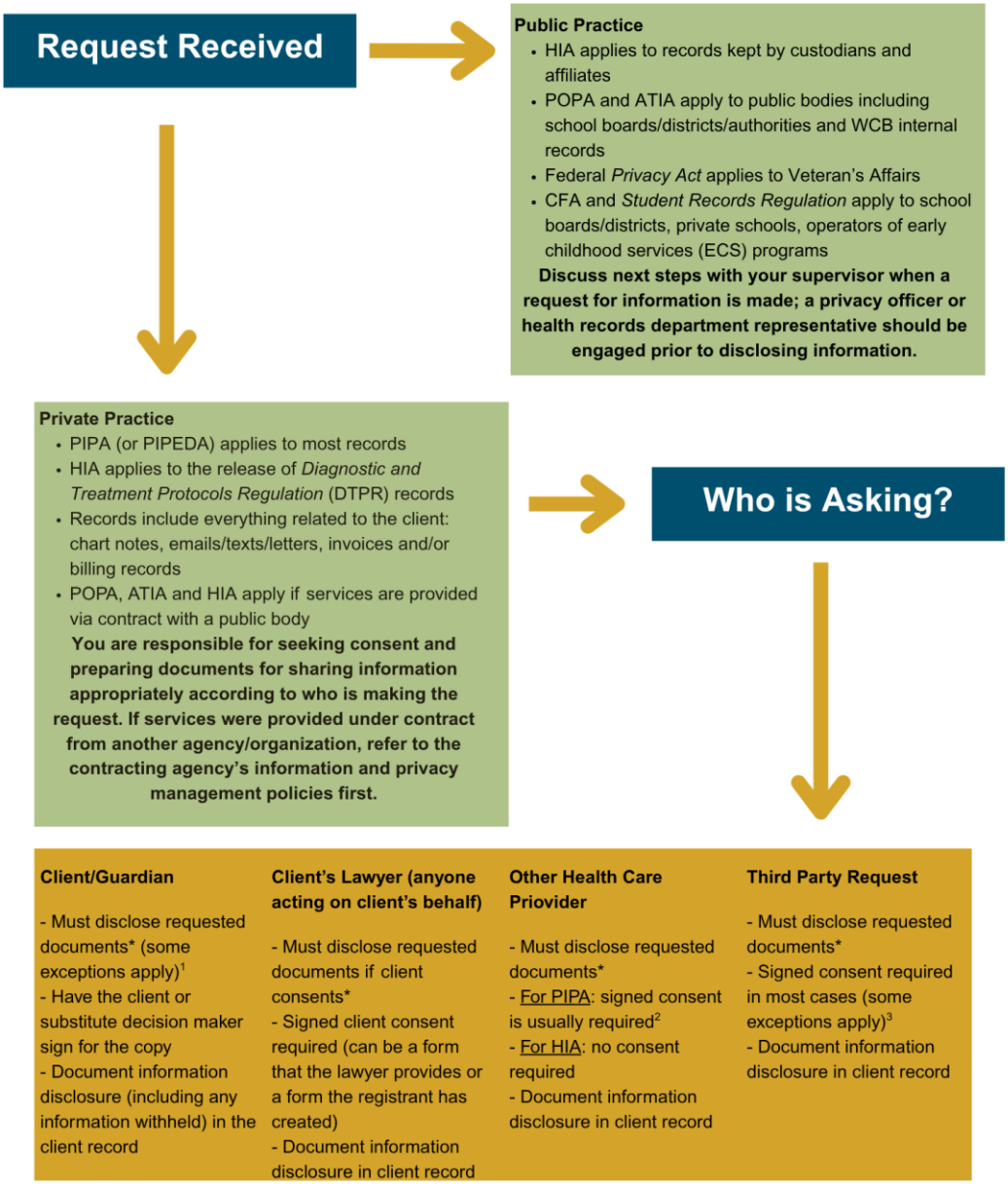
Appendix B – Which Privacy Legislation Applies

(Adapted from CLPNA's Privacy Legislation Flowchart)



Appendix C – Information Access and Disclosure Processes

(Adapted from Appendix F of CPTA's Privacy Guide)



* NOTE: PIPA allows for reasonable fees to be charged for preparing records for release (e.g. for printing electronic records or copying paper records); if a request for information is not addressed within 45 days, a client/guardian may file a complaint to the Office of the Information and Privacy Commissioner.

1 You can redact portions of a record if the information would reveal personal information about another individual; could threaten the life or security of another individual; or pose a threat to public safety. PIPA Section 24(3); HIA 11(1).

2 PIPA includes provisions that allow for disclosure of information without consent if the disclosure is in the interests of the client and consent cannot be obtained in a timely way, or if the individual would not be reasonably expected to withhold consent.

3 PIPA allows for the disclosure of information when required by a statute or regulation of Alberta. For example, the *Health Professions Act* does not require client consent if client records are requested by a regulatory body; HIA applies to DTPR records; and the Workers' Compensation Act, POPA and ATIA apply to WCB records.