

PIPA EMERGING ISSUES FEEDBACK

By Andrea Snow, Privacy Officer
College of Acupuncture of Alberta
College of Alberta Denturists

Thank you for providing us with an opportunity to provide feedback on potential changes to the Personal Information Protection Act (PIPA) in Alberta. Given that both regulatory colleges have fewer than six employees, we urge the government to carefully weigh the regulatory requirements to avoid imposing excessive red tape or administrative burdens on small organizations. It is essential to strike a balance that safeguards the privacy of Albertans while minimizing undue constraints on small businesses. This is also vitally important to the health professionals we represent as they operate small businesses.

Numbering does not align with the emerging issues document as number one introduces the subject.

1. Changing Legislative Landscape

- a. Are there specific amendments needed to harmonize PIPA with other jurisdictions to make it easier for businesses to operate in all jurisdictions? *This is not applicable to Alberta regulatory bodies.*
- b. Are there specific amendments to PIPA needed to modernize the Act for relevant businesses and organizations to conduct business in Alberta? *There may be an opportunity to address cross-border data transfers (outside Alberta/Canada/Internationally) by providing specific and clear guidelines for organizations wishing to engage third party service providers. All other opportunities are already identified within the issues document and are addressed below.*

2. Artificial Intelligence

- a. Should PIPA include a framework to regulate the design, development, and/or use of artificial intelligence systems within Alberta? *The current legislation should be modified to adapt to rapidly changing technology such as AI systems. If so, what should be included? The framework should regulate the design and development of AI systems and the use of these systems in Alberta with a focus on providing services that create a benefit to Albertans. Generally, the European Union Council and Parliament¹ comprehensive framework is a good start until more is known.*

¹ establishes obligations for AI based on its potential risk and level of impact • bans applications that are a potential threat to citizens' rights and democracy • permits specific targeted uses of biometric identification systems for law enforcement purposes • defines obligations for high-risk AI systems (that is, risks to health, safety, fundamental rights, environment, democracy and the rule of law) • establishes guardrails for general AI systems (i.e., Chat GPT and other models) • promotes measures for regulatory sandboxes and real-world testing of AI solutions without undue pressure from industry giants • defines sanctions for non-compliance

PIPA EMERGING ISSUES FEEDBACK

By Andrea Snow, Privacy Officer
College of Acupuncture of Alberta
College of Alberta Denturists

3. Application (non-profit, political parties)
 - a. Should all non-profit organizations be fully subject to PIPA for all their activities? *All personal information should be protected regardless of whether it is collected for a commercial purpose. Consider adopting GDPR approach in this regard.*
 - b. Should PIPA apply to political parties? *Similar to above, all personal information should be protected, and political parties should not be exempt.*
 4. Protections of Sensitive Personal Information (sensitive, biometric, children)
 - a. Should provisions be added to PIPA to further protect potentially sensitive information? *This is a huge gap. If so, for which information? Consider including categories like the GDPR such as sexual orientation, as well as biometric information.*
 - b. Should provisions be added for biometric information? *Yes, as this could include facial images that could lead to an identifiable individual.*
 - c. Should provisions be added to enhance the protection of children's personal information? *The current provision under s.61 seems sufficient.*
 5. Consent Requirements (plain language)
 - a. Are the provisions in PIPA dealing with forms of consent and the conditions attached to their use appropriate? *The current provision seems sufficient.*
 - b. Should individuals receive notice in plain language when organizations explain the purposes for which personal information is collected, used or disclosed? *Yes, plain language will enhance understanding and increase accessibility.*
 6. Individual Rights that are not included under PIPA (erasure, portability, automated decision systems)
 - a. Should PIPA include other protections for individual information, such as an individual's right to be forgotten or de-indexed? *See item 7.*
 - b. Upon an individual's request, should organizations be required to transfer that individual's digital personal information to another organization in a structured, commonly used, and machine-readable format when it is technically feasible (portability)? *This appears to create a financial and administrative burden on businesses and depending on the technology used to transfer the information, could create a greater risk of privacy breaches.*
-

PIPA EMERGING ISSUES FEEDBACK

By Andrea Snow, Privacy Officer
College of Acupuncture of Alberta
College of Alberta Denturists

Consider keeping legislation the same, which allows an individual to access their information.

- c. Should organizations be required to provide individuals with the logic involved in automated decision making about that individual (algorithmic)? *Small organizations likely do not have the resources for this type of automation. Consider aligning with other legislation to ensure consistency.*
7. Safeguarding Personal Information (deidentification, privacy programs, personal information assessments)
 - a. Should PIPA regulate the de-identification and/or anonymization of personal information within the control of an organization and the subsequent use or disclosure of the de-identified or anonymized information?
Given that PIPA lacks a provision for this practice, while most of the organizations mentioned in the document have such provisions, it appears prudent to adopt this as a best practice. If so, how? Create a hybrid of CPPA and QPSA to create consistent rules for those organizations who operate throughout Canada. Not clear how this is enforced in other jurisdictions; however, consideration should be given to it being upon complaint and/or through an audit process.
 - b. Should organizations be required to have a privacy management program and provide written information about the program to individuals and the Commissioner? *While maintaining a privacy management program demonstrates responsibility and ensures clear adherence to legislative obligations, it can pose an administrative burden for small organizations. Should the government opt for a strategy akin to CPPA, it is essential to provide comprehensive guidance documents and support to all organizations in this regard. In relation to the disclosure of information about this program to individuals and the Commissioner upon request, it would be beneficial to require organizations to prominently display this information on their respective websites. This approach enhances transparency, reducing the administrative load associated with individually providing such information.*
 - c. Should organizations be required to complete and submit a privacy impact assessment to the Commissioner for specific initiatives involving personal information? *While privacy impact assessments are important, they would impose a significant administrative burden on small organizations. The provisions in the QPSA are sensible as they focus on the acquisition,*

PIPA EMERGING ISSUES FEEDBACK

By Andrea Snow, Privacy Officer
College of Acupuncture of Alberta
College of Alberta Denturists

development, or overhaul of information systems or electronic delivery systems involving personal information. This approach may also reduce efforts and costs down the road if the system(s) turn out to be non-compliant. Extending these requirements further would unduly burden small organizations.

8. Breach Notification

- a. Are the provisions for notification of breaches to the Commissioner and individuals under PIPA appropriate? *Currently, PIPA allows organizations to delay notifying individuals of a breach until directed by the Commissioner. However, this could lead to delayed action and increased harm if the Commissioner's response is not timely. To address this, we propose strengthening the language in PIPA to mandate organizations to notify individuals if they believe the breach poses a serious risk or harm. This adjustment aligns with similar provisions in other jurisdictions outlined in the document.*

9. Administrative Monetary Penalties

- a. Should PIPA include the ability of the Commissioner to levy administrative monetary penalties against an organization of certain contraventions of the Act? *Presently, the legislation requires the Commissioner to refer cases to the Crown for prosecution, a process that consumes significant court resources and leads to unwarranted delays. Granting the Commissioner authority in this regard would expedite proceedings and alleviate the burden on the courts. However, it is imperative to clearly define the scope of contraventions to which this authority applies. It should be limited to cases where businesses repeatedly cause serious harm to individuals and fail to implement the necessary protections. To ensure fairness, an appeals mechanism should be incorporated. Furthermore, to minimize court involvement, an administrative tribunal should be established for this purpose as commonly seen in other legislation.*