College of Midwives of Alberta	Written Submission: AB Health on PIPA	To: Standing Committee on Resource Stewardship AB Health Date: May 2024

The College of Midwives of Alberta (CMA) was invited to review *Emerging Issues: The Personal Information Protection Act* document from the Alberta Government Standing Committee on Resource Stewardship.

Thank you for addressing this very important area of health care. CMA supports the efforts of the Alberta Government to address privacy of personal information because of the fast-paced speed of technological advancement. Thank you for the *Emerging Issues* document, comparisons in summary and chart form various pieces of legislation from Europe and Canada.

Preamble

The CMA, as the health regulatory body for Alberta's Registered Midwives, considers itself a non-profit organization. Our role is protection of the public interest through regulation and we focus on the privacy of information of the following groups:

1. CMA Registered Midwives' Clients: CMA regulates its registrants on privacy of personal client information through the *CMA Code of Ethics, Standards of Practice, Alberta Competencies for Midwives, CMA Bylaws, Governance Policies* and additional CMA policies and guidance documents. The CMA receives minimal client personal information directly. The information received is primarily related to the professional conduct and complaints processes of our mandate.
   For the day-to-day management of personal client information, the CMA ultimately turns to and relies on our service provider partners to protect personal client information. Specifically, this is Alberta Health Services Provincial Midwifery Administration Office, their work with AHS acute care and their service contracts with midwifery practice groups. The midwifery practice owners are responsible for management of personal client information for those clients in midwifery care.
2. Registered Midwives' personal information: The CMA is concerned with privacy of personal midwifery information through our registration, competence and professional conduct areas of responsibility.
   a. CMA receives registration applications from midwives who are educated and practicing in countries all over the world. We consider ourselves part of the Global Community.

b. CMA maintains a public register listing all registered midwives with the CMA, their registration status, their work contact information and their professional conduct status.

For CMA, from an Artificial Intelligence (AI) standpoint, the world is now the stage, not just single countries or continents. One sobering truth that CMA grapples with is that the use of AI is only as good as the humans prompting, managing it and adhering to any "rules" around privacy of personal information - past, present and future. Yet, legislation addressing privacy of personal information is possibly one of the only ways to guide AI use. CMA supports strong, clear rules, with a healthy wariness for humans being consistently ethical. There must be an equally strong societal system operating to safeguard against unethical people – human scammers, opportunists and those who want to gain from the victimization of other humans.

The following content is the Written Submission comments and recommendations from the CMA. CMA has addressed the questions posed in the *Emerging Issues* document by section.

Section 1.0 Introduction

1.2 CMA supports your work done on identifying emerging issues. Thank you for supplying this.

Section 2.0 The Changing Legislative Landscape in Canada and Internationally.

Questions:

1. *Are there specific amendments needed to harmonize PIPA with other jurisdictions to make it easier for businesses to operate in all jurisdictions?*
2. *Are there specific amendments to PIPA needed to modernize the Act for relevant businesses and organizations to conduct business in Alberta?*

Language definitely needs to be added to PIPA around non-profits, to harmonize with European Union (EU), Quebec and BC legislation. Please see the CMA preamble above for where CMA sees itself as a regulatory body organization on the world stage. We favour the EU/GDPR approach in this matter, and that Bill C-27, CPPA and AIDA need to expand language to match. It sounds like BC and Quebec are attempting to address stronger language to protect privacy of personal information. Personal information must also be clearly defined, to provide context and understanding.

Section 3.0 Artificial Intelligence

Thank you for defining Artificial Intelligence; this gives a context for further consideration.

Question:

Should PIPA include a framework to regulate the design, development, and/or the use of artificial intelligence systems within Alberta? If so, what should be included?

Yes, PIPA should include a framework to regulate the design, development and use of AI systems. Again, we favour the EU/GDPR *Artificial Intelligence Act* approach in this matter. The Office of the Privacy Commissioner of Canada (OPCC)with its AI appropriate laws also appears to be on the same pathway. AIDA has a good start but needs stronger language and more detailed considerations.

One advantage for PIPA is that it uses technologically neutral language for specific types of records or technology, allowing application to personal information, but this could also be interpreted differently from the intended purpose, unless spelled out explicitly.

Section 4.0 Application

Questions:

1. *Should all non-profit organizations be fully subject to PIPA for all of their activities?*

PIPA does include a number of entities; CMA would like to see non-profits clearly included in the list and for those organizations to follow the same rules (section 56 reconfigured) as those listed under PIPA.

Again, the GDPR includes all organizations, including non-profit, and BC and Quebec proposals appear to include non-profits as well.

2. *Should PIPA apply to political parties?*

Although outside of the CMA sphere of influence, political parties should be included under these same rules.

CMA did not fully consider any downside analysis of the impact of the changes introduced in the above questions. The criminal system may be the one to carefully consider exemptions.

Also, CMA did have a question regarding the HIA and how this relates to PIPA and if there is one that supersedes the other. At the very least, PIPA should be consistent with BC and Quebec and changes also need to be considered for the HIA and CPPA.

Section 5.0 Protections of Sensitive Personal Information

Questions:

1. *Should provisions be added to PIPA to further protect potentially sensitive information? If so, for which information?*

Yes, PIPA needs to add extra provisions. The GDPR sets out particular categories, including biometric data. CMA generally supports the use of these categories. One issue came up about religious or political beliefs being sensitive information. These are charter of rights issues and are not the same as people actually <u>acting</u> on those beliefs with damaging effects to other human beings. That is why the criminal justice system must have access to key information in this area.

Quebec's QPSA also includes s 8.1 protection against the person concerned being "*identified, located or profiled*" which should be included in potentially sensitive information.

2. *Should provisions be added for biometric information?*

Yes, as per above question. In addition to facial images, iris scans, voice recognition, fingerprint access systems, keystroke monitoring and geolocation are key considerations. Thank you for the GDPR definition of biometric data: PIPA should adopt this. We understand PIPA has consideration for these aspects generally, not sure if there is a need to further label or identify the biometrics……. Soon we will need to add DNA perhaps………

3. *Should provisions be added to enhance the protection of children's personal information?*

Yes, CMA "clients" include the fetus and newborn baby by definition.

Section 6.0 Consent Requirements

Questions:

1. *Are the provisions in PIPA dealing with forms of consent and the conditions attached to their use appropriate?*

We note Dr Teresa Scassa's comments on the balance of making meaningful consent and reducing the consent burden to enable greater use of data by private and public sector entities, for a goal of greater good. There are pros and cons to each aspect, and perhaps NO "happy medium". By definition, AI crunches large amounts of data and it also has the potential to use the data, as time goes by and sophistication improves, to negatively impact people. Consent processes need to be in place now.

PIPA needs to more clearly define this part, especially the "reasonable purposes", as this is a way for ill-intentioned entities to use the data in a negative way, perhaps harming people. Again, obtaining consent is only as good as the conditions and the people involved. We support the language of both GDPR and Quebec on this matter.

PIPA also needs to change the "express consent", "deemed consent" and the "opt-out consent" to the more clearly defined terms in the GDPR, and the QPSA.

2. *Should individuals receive notice in plain language when organizations explain the purposes for which personal information is collected, used or disclosed?*

CMA supports this, and also supports the language from the GDPR and from Quebec's QPSA. We cannot assume literacy levels of residents in Canada or Alberta, as we are multicultural and plain language can increase inclusivity, equity and accessibility.

Section 7.0 Individual Rights that are Not Included Under PIPA

Questions:

1. *Should PIPA include other protections for individual information, such as an individual's right to be forgotten or de-indexed?*

PIPA and CPPA could consider where an individual may require an organization to erase, dispose or de-index the personal information it holds about that individual. This practice may help to increase protection of personal information, especially when AI crunches large amounts of data. Clear definitions of "erasure" and "de-indexing" are needed.

There could be a downside to this ability, related to individuals intentionally wanting to be 'lost' from society. This questions brings up the concept of the capacity of individuals to "own" their personal information and the role of guardians etc, and how people could actually manipulate the processes to allow for de-indexing other individuals. In the case of sex offenders, or those who are convicted of harmful human and other (environmental) crimes, the criminal justice system would have to have exemptions to protection of certain personal information. Then there is the potentially corrupt criminal justice scenario…………..

2. *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 (data portability)?*

CMA has this ability now, through a consented "Letter of Standing" used interjurisdictionally in Canada. CMA likes the GDPR circumstance where individuals can obtain a copy of their personal data from a controller in a structured, commonly-used, machine-readable format. There are pros and cons to this, mainly related to the individual's ability to keep the data (not lose it) and to know how important the data is to produce at key points in time.

The QPSA approach seems to be much like how research is conducted, and has ethical grounds.

CMA also likes the "Rights-based" legislation of the GDPR and the QPSA where they are spelled out, and PIPA needs to incorporate these clearly, especially the logic behind the ADS, and portability for data.

3. *Should organizations be required to provide individuals with the logic involved in Automated decision-making about that individual (algorithmic transparency)?*

Thank you for providing the concept of algorithmic transparency. Thank you also for the CPPA definition of ADS (Automated Decision System) as "*any technology that assists or replaces the judgement of human decision-makers through the use of rule-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other techniques."* Generally, it is always wise to inform individuals about their personal information. The GDPR approach again seems like a thoughtful and logical way to inform individuals about the possibility of ADS. A disclosure statement may also be helpful; in the instances where AI will be used to generate data inferences. This is also cumbersome and time consuming for communication and consent.

Some situations would be amenable to the ADS, to make life easier for those decision-makers involved and perhaps even be safer. However, not all situations are able to fit into or be repurposed into this ADS format – like childbirth, for example, or the human body and its nuances. People are not machines. Personal data used for AI use may NOT be helpful. Again, it depends on the definitions of "Helpful".

PIPA should adopt language around this to align with the GDPR.

Section 8.0 Safeguarding Personal Information

Questions:

1. *Should PIPA regulate the de-identification and/or anonymization of personal information within the control of the organization and the subsequent use or disclosure of the de-identified or anonymized information? If so, How?*

"De-identification' and "anonymization" should be clearly defined to establish a base for consideration. The definition of "anonymization" in the paragraph under 8.1 is such a definition. QPSA has a starting definition "de-identification". Not sure how effective policing will happen for organizations around destruction of information when an organization has achieved its purpose for collecting or using personal information. PIPA states that an organization must make "reasonable" security arrangements; CMA believes this needs to be strengthened to a maximum level and delete "reasonable". CMA would support changing CPPA processes of de-identifying to be stronger as well. The GDPR has a great rule and concept for processing "Pseudonymized data". This would be an approach for PIPA to consider.

2. *Should organizations be required to have a privacy management program and provide written information about the program to individuals and the Commissioner?*

Yes. The description in PIPA and in the CPPA is used by Midwifery Practices for compliance with the Acts. This is carried out in the CMA as well, with Governance Policies addressing privacy and confidentiality of information. The GDPR approach is one step further and clearer, including outcome measures. QPSA adds even more by publishing on the organization's website how personal information is managed. That sounds wise.

3. *Should organizations be required to complete and submit a privacy impact assessment to the Commissioner for specific initiatives involving personal information?*

Yes, the notion of a privacy impact assessment is a good one, and PIPA should adopt that. If the Commissioner is an appropriate place to submit the assessments to, that should be done as well. Are there people to monitor these assessments and processes? CMA is very cautious about the CPPA portion of Bill C-27 for use of a PIA for exemptions to consent. The conditions sound "reasonable" but enforcing the use of and processes related to are very hard to do.

Section 9.0 Breach Information

Question:

> *Are the provisions for notification of breaches to the Commissioner and individuals under PIPA appropriate?*

Generally-speaking, yes. Timeframes are always hard to define, but GDPR and QPSA do that. PIPA could pattern language after the GDPR. Some of the provided information indicates that the number of reported breaches is increasing, suggesting more breaches are occurring overall. This is concerning, and effective measures need to be taken.

Section 10.0 Administrative Monetary Penalties

Question:

> *Should PIPA include the ability of the Commissioner to levy administrative monetary penalties against an organization for certain contraventions of the Act?*

Serious issues require serious penalties. Examples from the GDPR and QPSA can benchmark targets for PIPA. If the Commissioner is able to levy these, that would be easier to administer and avoid court time. The "to promote compliance" approach is again, too "Canadian" and lenient, and will not be taken seriously by the rule breakers.

CMA supports the addition of the QPSA phrase "natural person" if it can be defined well, so that the penalties are levied against humans/people, not AI systems.