Association of Ontario Midwives
Delivering what matters.

August 10, 2017

Eric Sutherland
Director – Information Management Strategy and Policy
Health System Information Management Division
Ministry of Health and Long-Term Care
13th Floor, 1075 Bay Street Toronto, ON M5S 2B1
eric.sutherland@ontario.ca

Dear Mr. Sutherland:

Re: Health Information Protection Act Regulations

Thank you for the informative presentation at the Coalition of Ontario Regulated Health Profession Associations (CORPHA) meeting on July 20, 2017 and for this opportunity to provide feedback for the development of regulations for implementation of the Health Information Protection Act.

Midwives in Ontario, as primary care providers, are health information custodians under the Personal Health Information Protection Act. A number of midwives currently use an electronic health record (EHR) in their clinic, many midwives use EHRs in the hospitals where they hold privileges, and soon most midwives will have access to the Ontario Laboratory Information Service (OLIS). The Association of Ontario Midwives (AOM) is also working with BORN Ontario to propose to the Ministry that all midwifery practice groups have EHRs in their clinics within the next five years. Additionally, all midwives enter data into the Better Outcomes Registry Network (BORN Ontario). This letter shares some of the privacy issues that have arisen for midwives that warrant consideration in the development of these new regulations, especially as EHRs become increasingly integrated, with access by a greater number of users at more sites.

Informed choice is the basis of the model of midwifery practice in Ontario. Within this model, like other models of patient-centered care, the client is empowered to make the decisions that they deem are best for them and their baby. Midwives build a relationship of trust with their clients, provide evidence-based information and professional opinions, and participate in shared decision making with their clients. The majority of our questions and comments in this letter centre on the process and the integrity of informed choice for clients/patients:

- We assume that data-masking will be one of many systems to protect patient privacy and ensure that healthcare providers are not inappropriately accessing patient information. Snooping is an issue in institutional EHRs, which requires rigorous audit systems, training, and access restrictions to address. These risks grow exponentially

with a provincial system, as both the number of healthcare providers with access grows and the number of patients in the EHR grow. It would be impractical and inappropriate to put the onus on individuals to mask their data from every possible snooper. Instead, the EHR itself needs to have rigorous and redundant systems to protect patient privacy and foreclose inappropriate access.

- From an informed choice perspective, patient consent directives should be meaningful and accessible, especially to the most vulnerable patients. This means ensuring that all patients know that there is an EHR, what data it will contain, who can access it, and what steps can be taken limit access (i.e., masking). This knowledge should not be assumed.

  Further, the process for masking and unmasking data should be clear to patients and not overly cumbersome that it would deter a patient from masking data. When patients call eHealth Ontario to discuss masking their data, we recommend that a health professional should be available to engage in a personalized discussion with the patient about the potential implications of masking certain information (including potential delays in accessing comprehensive care, greater potential for error, and negative impacts to the relationship of trust between patient and provider).

- We are concerned that how masked data appears in the record may impact the relationship of trust between patient and healthcare provider.

  For example, an Indigenous patient may wish to have records masked that incorrectly make a diagnosis of alcoholism in order to avoid further stigmatization and poor healthcare. At present, this patient would be able to avoid that stigmatization by not sharing this incorrect history. However, in an integrated EHR, a healthcare provider might see that some data is masked and make assumptions about the patient's history and what information is masked. Having healthcare providers know that information is masked may undermine the patient's objective in having that information masked.

  As a result, we recommend that how the existence of masked data appears be carefully considered. Depending on its appearance, we recommend education of providers be provided regarding the reasons why patients might want to mask some of their health record.

- We understand the need to have non-maskable data for the accurate identification of the correct patient record. However, at times it may be warranted to also mask the address field. For example, we are aware of a situation of a midwifery client fleeing an abusive relationship who feared for their safety if their abusive partner could have accessed this information through an EHR. In these situations, the inability to mask the address field could create a significant safety issue. Moreover, if people experiencing violence know that their address cannot be masked, they may be more reluctant to access the health care that they need.

To facilitate the identification of the correct patient record, especially for those without an OHIP number, we recommend a field for another identifying health number (such as the Interim Federal Health Plan) be included and be non-maskable.

- As healthcare providers have professional responsibilities for record-keeping, we assume that even if a record was blocked by patient request, the creator of the record would always have access to it. This is important for the purposes of accountability and quality improvement. It is our understanding from the briefing that the creator would always have access to the record, and we support this.
- Date-based masking could be an appropriate additional level of granularity to allow patients to conceal a period of time or 'episode' that is not consistent with their general health and that has the potential to negatively affect their experience of care. We recommend providing this option to patients.
- It seems appropriate that the health information custodian who accessed the record would have a responsibility to notify the patient that their consent directive has been overridden and in the method (mail, e-mail, texting, etc.) chosen by the patient. They should also have an obligation to notify the patient at the first reasonable opportunity. We would also recommend that there be a central notification mechanism (e.g., from eHealth Ontario, again, in the method of the patient's choosing) to ensure patients are actually notified of an override as a safeguard against "snooping".
- The AOM is strongly opposed to the release of patient identifying data to the Ministry of Health and Long Term Care, or any branch of the government. Midwives and their clients will have grave concerns with the Ministry of Health, or any branch of government, having access to all the personal health information of Ontarians regardless of the internal ministry process and best intentions to de-identify data.

  Midwives have experienced this reticence to share information with an arms-length government agency first hand: midwives have received requests from clients to not enter their information in the BORN data system as they do not want their personal health information, or that of their newborn, to be accessible to those outside their circle of care. Healthcare providers may be put in the untenable position of having to choose between not charting the provision of healthcare and not billing for services provided; or of respecting their patient's privacy directions.

  Some Ontarians may be reluctant to access health care or to divulge information to their healthcare providers for fear of discrimination by government agencies. The most serious repercussion of providing personal health information to the provincial government, is that patients may not access needed health care, share their full medical history, or may seek anonymous health services (e.g., anonymous HIV testing). Patients who need treatment for or have had a history of drug and alcohol addictions, mental

health illnesses, sexual abuse, abortions, or sexually transmitted infections such as HIV, are most vulnerable in this regard.

As patient consent is a key component of privacy legislation, the Ministry may also wish to consider how patients can opt out of the central EHR; for example, maintaining alternative paper records and a method of billing outside of the EHR.

Thank you for this preliminary opportunity to provide feedback. We look forward to reviewing the draft regulations when they are released. Should you have any questions, please do not hesitate to contact us.

Sincerely,

Elizabeth Brandeis, RM, BHSc, MScCH
President

Kelly Stadelbauer, RN BScN MBA
Executive Director