SUBMISSION OF THE INFORMATION AND PRIVACY COMMISSIONER

The submission of the Information and Privacy Commissioner to Ed Clark, whose has been tasked with assessing the value of Ontario's digital health program, will emphasize three main points:

1. The province has a comprehensive framework for the protection of privacy of Ontarians in the electronic health record, which has been passed and is awaiting proclamation;

2. Great caution should be exercised prior to any consideration of the monetization of the personal health information of Ontarians in the electronic health record; and

3. Ontarians must be empowered to play a greater role in their own health care by providing them with direct access to their personal health information.

1. A COMPREHENSIVE PRIVACY FRAMEWORK ALREADY EXISTS IN ONTARIO

In Ontario, the privacy of individuals and the confidentiality of their personal health information is protected by the *Personal Health Information Protection Act* (*Act*). The *Act* is a consent-based statute, meaning, persons and organizations in the health sector, defined as "health information custodians," may only collect, use and disclose personal health information with the consent of the individual to whom the information relates, subject to limited exceptions set out in the *Act*. This legislation was the culmination of years of extensive consultations with a broad range of stakeholders, including patient groups, regulatory colleges, associations of health professionals and researchers.

My office is charged with overseeing compliance with the *Act*. After more than a decade, I can attest to the fact that the *Act* strikes the right balance between protecting the privacy of Ontarians, and the equally important objective of ensuring the continued delivery of effective and efficient health care. It also facilitates the use of health information for secondary purposes that are in the public interest, including research, analysis and planning for our publicly funded health system. The *Act* has also served as a model for health privacy legislation in many provinces and territories, providing for greater harmonization of privacy protections across our nation. Most importantly, the *Act* meets the public's expectations around the protection of their personal health information.

The *Act* was recently modernized to facilitate the implementation of the provincial electronic health record with the passage of Bill 119, the *Health Information Protection Act, 2016*. When proclaimed, Part V.1 of the *Act* will address the rights of individuals and the duties and obligations of health information custodians (custodians) in the provincial electronic health record and ensure that health information accessible by means of the provincial electronic health record is available for secondary purposes, subject to necessary and appropriate safeguards. To enhance harmonization of privacy protections across our province, all three shared regional systems, including ConnectingGTA, are being developed and implemented in accordance with the privacy framework set out in Bill 119.

I urge the government to proceed with its proclamation as soon as possible to ensure harmonization of privacy standards across the province.

2. GREAT CAUTION SHOULD BE EXERCIZED PRIOR TO MONETIZATION

Role of eHealth Ontario

Before contemplating monetization, it is important to consider who has custody and control of the personal health information accessible by means of the provincial electronic health record.

eHealth Ontario is not a custodian under the *Act*. eHealth Ontario is an electronic service provider whose role is to provide services to custodians to enable them to use electronic means to collect, use and disclose personal health information. Since it is not a custodian, *eHealth Ontario does not have custody or control of personal health information*. Custody and control rests with the custodians of the information and, in almost all shared electronic health record systems, custody and control is shared among the custodians who create and contribute personal health information to the systems.

eHealth Ontario is subject to strict duties and obligations under section 6 of Regulation 329/04 to the *Act*. For example, eHealth Ontario is prohibited from using personal health information except as necessary in the course of providing services to custodians. This means that eHealth Ontario cannot de-identify, for its own purposes, the personal health information to which it has access in the course of providing services. eHealth Ontario may only de-identify personal health information as authorized by custodians and for the purposes of the custodians. Further, eHealth Ontario is prohibited from disclosing personal health information for any purpose. Any third parties retained by eHealth Ontario are subject to these same strict duties and obligations.

In addition, if eHealth Ontario is designated as a prescribed organization in respect of the provincial electronic health record, it will be subject to similar duties and obligations under Part V.1 of the *Act*. As a prescribed organization, eHealth Ontario and the third parties it retains would also be under an obligation to limit the receipt of personal health information to that which is necessary to develop and maintain the provincial electronic health record.

Requirement for De-Identification

Should the government wish to proceed to monetize personal health information, it must first be de-identified. As noted above, the legal authority to de-identify personal health information rests with the custodians of the information, and not eHealth Ontario. To be de-identified within the meaning of the *Act*, the information must not identify an individual directly or indirectly, meaning, it must not be reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual.

De-identification of complex, multi-dimensional and longitudinal information for purposes of monetization, including the de-identification of personal health information, presents many practical, technical and operational challenges and risks to the privacy of Ontarians that must be properly mitigated and addressed. De-identification requires the management of risks associated with both direct identifiers (e.g. name, address, health card number and medical record number) and indirect identifiers (e.g. gender, date of birth, postal code and date of receipt of health services). De-identification is particularly challenging in the context of personal health information given the number of direct and indirect identifiers, the amount of detail contained, and the fact that each individual's health care experiences are unique. It is also challenging because de-identification

must take into account the circumstances of the disclosure, including to whom the information will be disclosed, the purposes for which it will be disclosed, the restrictions on subsequent uses and disclosures, and other mitigating controls that will be imposed.

It is important to note that de-identification does not reduce the risk of re-identification to zero. In the context of monetization, personal health information would need to be de-identified to such an extent that the risk of re-identifying an individual would be extremely low. It is also important to note that there is an inverse relationship between de-identification and data quality. The more de-identification applied, the lower the quality of the information and the less value it has for secondary purposes.

In addition to the challenges posed by de-identification, there are a number of ethical considerations that must be addressed prior to any monetization, including the public interest in monetization and the public interest in the subsequent uses and disclosures of the de-identified information.

Potential Unintended Consequences of Monetization

Personal health information is one of the most sensitive types of information. It is not only highly private and personal, but goes to the integrity and autonomy of the individual. In the course of seeking treatment and care, Ontarians provide this information to their health care providers with whom they have a relationship of trust and confidence on the basis of implied consent. The implied consent model is integral to the legislated framework for the protection of personal health information in this province. It protects the privacy of individuals and the confidentiality of their personal health information while, at the same time, facilitating the safe and effective provision of health care.

Any movement towards monetizing personal health information, even in de-identified form, may impact the fiduciary relationship between individuals and their health care providers and may give rise to unintended consequences. For example, if patients are concerned about the subsequent uses and disclosures of their personal health information, including the monetization of their de-identified information, they may avoid seeking necessary treatment; they may withhold information that is needed to provide safe and effective health care; or they may provide inaccurate or misleading information. In addition, health care providers may avoid recording accurate, complete and up-to-date information in electronic health record systems and may be reluctant to participate in shared electronic health record systems due to concerns over monetization. As a result, monetization may stall the already slow progress of digital health in this province.

Requirement for a Legislated Framework for De-Identified Information

Should the government wish to proceed to de-identify the personal health information of Ontarians for such purposes, in our view, broad public consultation and a comprehensive legislated framework would be required. At a minimum, the legislated framework must:

- Identify from whom the personal health information will be collected for such purposes;

- Identify the person or organization responsible for collecting the personal health information and for de-identifying the information;

- Require that the responsible person or organization immediately de-identify the personal health information upon its collection;

- Set out the de-identification procedure that the responsible person or organization is required to follow;

- Require de-identified information to be reviewed prior to its disclosure to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual;

- Identify the person or organization responsible for reviewing the de-identified information prior to its disclosure and the process that must be followed in this regard;

- Establish the criteria that be must be used to assess the risk of re-identification;

- Identify the persons or organizations to whom de-identified information may be disclosed;

- Identify the purposes for which the de-identified information may be disclosed;

- Impose restrictions on the subsequent uses and disclosures of the de-identified information;

- Prohibit the use of the de-identified information, either alone or with other information, to identify an individual;

- Set out the other mitigating controls that will be imposed on persons or organizations to whom the de-identified information is permitted to be disclosed;

- Establish independent privacy and ethical oversight in order to ensure that the privacy of individuals is protected and that the de-identified information is used in the public interest and not in a manner that stigmatizes or discriminates against an individual or group of individuals;

- Require transparency with respect to all the matters set out above; and

- Establish penalties and sanctions for failing to properly de-identify personal health information, for using or attempting to use de-identified information to identify an individual, for failing to adhere to restrictions on subsequent uses and disclosures of

the de-identified information and other mitigating controls, and for contravening the legislated framework.

3. NEED FOR SECURE DIGITAL TECHNOLOGIES TO ENABLE PATIENT ACCESS

In February 2015, the Ministry of Health and Long-Term Care published *Patients First: Ontario's Action Plan for Health Care* in order to transform the health system into one that puts the needs of patients at its centre. One way to put the needs of patients first is by providing them with the information needed to make decisions about their own health care. For this reason, it is imperative that once personal health information has been integrated into the provincial electronic health record, patients are enabled to access their information as well as other health services through convenient and secure digital technologies. It is, after the patient's information. When proclaimed, Bill 119 will enable the Lieutenant Governor in Council to make regulations enabling such access and services.