Building Ontario's Next-Generation Smart Cities Through Data Governance

Part 1: Health Data Safe Haven

Recommendations for improving access to health data to support communities

I. ABOUT THE SERIES

Building Ontario’s Next-Generation Smart Cities Through Data Governance

There are many definitions of a “smart city,” but central to all of them is the implementation of advanced technology for the creation of systems and services to support prosperity and quality of life for people. As cities adopt smart infrastructure, they are beginning to gather useful data. Alone, that data can provide useful insights to help make specific aspects of city life more efficient and more livable. Combined with other data, city data could generate innovative new uses and new value. This emerging opportunity raises important questions on how data might be owned, shared and governed.

It’s still early days and cities around the world are still figuring it out, researching and testing new methodologies, and leveraging digital technologies to support them. In such environments, digital research infrastructure is key to the exploration of smart cities data governance.

Rapid advancements in data collection, transfer, and analysis technologies have provided the Government of Ontario with the opportunity to explore new infrastructure systems for economic development. These technologies have enhanced the government’s ability to amass volumes of data and interpret them to create data-driven solutions to challenges in infrastructure development and delivery of products and services to the citizens. However, this also raises concerns around privacy, security, individual rights, and privatization of citizen data. In order to balance innovation that leverages this data with individual wellbeing, the Government of Ontario granted Compute Ontario and ORION funding to study smart cities.

To support this deep-dive into smart cities and data governance models, Compute Ontario and ORION convened diverse stakeholders and experts from policy and governance sectors, as well as industry, academia, and research. We brought over 125 stakeholders together at a “Smart Cities Governance Lab” in Kitchener, Waterloo, in March 2019 to discuss and workshop the topic, and assembled a “Smart Cities Advisory Committee” with whom we regularly consulted. The committee brought diverse representation and expertise that informed our areas of exploration, and validated report recommendations. Through three use case studies, we further explored data governance in areas health, personal mobility, and open data architecture to facilitate more equitable access to the data market and enhance economic development within the province.

This series of reports is a culmination of these efforts and focuses on resulting recommendations, existing examples of data governance models, and exploring various data principles, commons, collaboratives, and trusts.

We begin the series with a report from the Institute for Clinical Evaluative Sciences (ICES) that explores building a data trust to improve access to health data for a broader group of stakeholders to support communities.

ACKNOWLEDGEMENT

ICES would like to thank Compute Ontario and ORION for guiding this work as part of the smart cities data governance report supported by the Government of Ontario.

TABLE OF CONTENTS

I. ABOUT THE SERIES

II. THE PROJECT

Introduction to ICES

Exploring the Health Data Trust Model

III. RECOMMENDATIONS

ICES as a Data Safe Haven

Principles—Data Governance and Ethnical Use Framework

Economic Potential

Appendix

Glossary

Term	Definition
CO	Compute Ontario
DQIM	Data Quality and Information Management
FIPPA	*Freedom of Information and Protection of Privacy Act*
FNIGC	First Nations Information Governance Centre
HIC	Health Information Custodian
ICES	Institute for Clinical Evaluative Sciences
IKN	ICES Key Number
IPC	Information and Privacy Commissioner of Ontario
MEDJCT	Ministry of Economic Development, Job Creation and Trade
MFIPPA	*Municipal Freedom of Information and Protection of Privacy Act*
MOHLTC	Ministry of Health and Long Term Care
OCAP	Ownership, Control, Access and Possession
PAC	Public Advisory Council
PE	Prescribed Entity
PHI	Personal Health Information
PHIPA	*Personal Health Information Protection Act, 2014*
PI	Personal Information
PIA	Privacy Impact Assessment
PIPEDA	*Personal Information Protection and Electronic Documents Act*
PLO	Privacy and Legal Office
REB	Research Ethics Board

List of Tables and Diagrams

II. THE PROJECT

The Team

Rosario G. Cartagena, Chief Privacy and Legal Officer, ICES

J. Charles Victor, Senior Director, Strategic Partnerships and External Services, ICES

Kelley Ross, Senior Privacy Advisor, ICES

Emily Scrivens, Privacy Analyst, ICES

Michael J. Schull, CEO, ICES

Disclaimers

ICES is not subject to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)[1] which protects the privacy of personal information for the collection, use and disclosure by municipalities and municipal institutions. Therefore, this report does not address whether as part of the Smart Cities initiative, municipalities can disclose personal information to ICES for any analytical insights. The Report is written solely from the perspective of ICES' ability to provide greater access to its data repository.

Any data or processes referenced herein does not include data where ICES has been named as a data steward by its Indigenous partners.

[1] *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56. [MFIPPA]

Executive Summary

Foundational privacy laws in Canada, including those related to secondary use of data are built around the idea of individual data, and do not generally include any notion of collective data rights.[2] On the other hand, data and research institutes have the ability to generate analyses and insights from data collected as well as help inform decision and policy-makers on effective and efficient health care systems and delivery. ICES is one of the few organizations in Ontario to collect and use personal health information without consent from health information custodians for the secondary purposes of health system planning and monitoring. It can also disclose personal health information for research purposes as set out in legislation. However, its ability to disclose personal health information or even de-identified information for wider purposes or even to varying actors in the system is limited legislatively.

Although a trust may convey the notion of stewardship more so than other legal structures, the trust relationship sought to be attained by a trust model is, in Canada, already legally present for all corporations that are registered charities. Further as described in this report, our finding is that a trust has no standing under Ontario's current public sector and health sector privacy laws to receive and collect personal health information and is in no better position than ICES to allow broader access to data. Ultimately, legislative amendment must take place for data including de-identified data, to be disclosed by ICES for non-research purposes - where research ethics board oversight is not the appropriate vehicle. Indeed, it may be that instead of a research ethics board model which is limited to instances where data is to be utilized for research purposes, another model for secondary use is warranted. Such data governance model would be built on ethical uses of data, but also include traditional data use principles such as privacy and security. Enabling a data governance and ethics framework would complement the legislative reforms described in this report and help to provide Ontarians with greater social acceptance for any data use related to Smart Cities.

[2] Bianca Wylie, "Open Data Endgame, Countering the Digital Consensus" (August 2018) 186 CIGI Paper.

Summary of Suggested Opportunities for Economic Realization

The amendments set out below would allow for a Data Safe Haven such as ICES to provide broader access to PHI or de-identified data, and enable greater economic potential in Ontario.

	Regulatory Amendments – Options
1	ICES to be named as a health data institute in PHIPA regulations for onward disclosures to third-parties such as researchers or others, to facilitate broader access and economic development, including innovation
2	PHIPA and FIPPA (and possibly MFIPPA) to be amended to clearly permit ICES to de-identify PHI for the purposes of onward disclosure to third-parties as part of evidence based-policy making or other broader purposes set out by the government
3	FIPPA to be amended to clearly permit ICES to collect and use PI (non-health data) for wider system planning and evaluation (evidence-based policymaking)
4	MFIPPA to be reviewed to assess whether ICES can collect and use PI (non-health) data for municipal system planning and evaluation (evidence-based policymaking) and if not, to amend accordingly
5	PHIPA and FIPPA to be amended to enable a ministry disclosing PI to allow ICES to collect and link the PI with PHI, and disclose the linked dataset to third parties, whether they be academics, policy-makers, HICs, MOHLTC, or other Ministries

Introduction to ICES

Background

The Institute for Clinical Evaluative Sciences (ICES) is an independent publicly-funded research and data organization established in 1992. ICES provides the Ontario government, health system stakeholders and researchers with access to high-quality, timely, and relevant health data and rigorous analytics, resulting in evidence that makes Ontario's health system stronger, policy better, and Ontarians healthier.

ICES has grown to be a network spread across seven (7) physical sites in Ontario, within universities and academic health science centres, supporting high quality health data research across the province. These sites create an opportunity for scientists to access ICES' data holdings from remote locations, build research capacity throughout the province, and foster closer connections with local partners for a more effective exchange of knowledge and evidence.

Legal Framework

ICES is a not-for-profit corporation under the *Corporations Act*.[3] The Articles of Incorporation set out the objects of the corporation, which include among others, "to establish and operate a research institute for the purpose of contributing to the quality, effectiveness, efficiency and equity of health care services in Ontario." ICES is governed by a board of directors pursuant to its by-laws.

Further, ICES has been designated as a Prescribed Entity (PE) under the *Personal Health Information Protection Act, 2014* (PHIPA).[4] This designation permits a Health Information Custodian (HIC)[5] to disclose to ICES, Personal Health Information (PHI)[6] for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services (Health System Planning).[7] This means that HICs can disclose PHI to ICES without patient consent for the purposes of Health System Planning.

In order for ICES to continue to collect and use PHI from a HIC for Health System Planning under PHIPA, the following must be met:[8]

[3] *Corporations Act*, R.S.O. 1990, c. C.38

[4] *Personal Health Information Protection Act*, S.O. 2004, c. 3, Sched. A [*PHIPA*]

[5] *PHIPA*, Ibid at s.3 (1). HICs include: a health care practitioners; hospitals, long-term care homes, retirement homes, pharmacies, laboratories, ambulance services, the Ministry of Health and Long-Term Care.

[6] PHIPA, *Ibid* at s.4(1)

[7] PHIPA, *Ibid* at s.45(1)

[8] PHIPA, *Ibid* at s.45(3)

- ICES must have in place practices and procedures to protect the privacy of the individuals whose PHI it receives and to maintain the confidentiality of the information; and

- the Information and Privacy Commissioner of Ontario (IPC) must approve such practices and procedures.

As a result, every three years, the IPC reviews ICES' privacy and security policies and procedures, templates, logs, human resources and other organizational practices. The IPC must approve ICES' practices and procedures in order for ICES to continue being designated as a PE for another three years. This rigorous oversight by the IPC has enabled ICES to be a trusted steward of 18 billion records for over 20 million Ontarians'– including all health card holders, past and present, (ICES Data Repository) and a global leader in secure access to data.

Further, although ICES does not have a designation under the *Freedom of Information and Protection of Privacy Act*[9] (FIPPA) - which governs Personal Information (PI), if the party who wishes to disclose PI to ICES is governed by FIPPA, then the disclosure and use by ICES must be in accordance with FIPPA. This is also the case if ICES collects data under the Federal *Privacy Act*.[10]

ICES is also a steward of Indigenous data (First Nations, Métis and Inuit people or communities)[11] to enable Indigenous-driven analyses using Indigenous and ICES data. Indigenous data governance and engagement is nuanced and complex. In each instance where Indigenous data is proposed for use, there are many things to consider and the landscape is evolving. ICES continues to develop data governance agreements with Indigenous partners and will apply Indigenous centered approaches to data use, for example, the First Nations principles of Ownership, Control, Access and Possession of First Nations data (OCAP) as necessary.

ICES Data Repository

The ICES Data Repository holds primarily administrative health service records for all Ontarians who are eligible for universal health coverage. Administrative health data sets are derived from the interactions individuals have with the health system and can therefore, be used to monitor and evaluate health care services. Further, these data sets include data elements on a variety of attributes critical to the health care system such as hospital discharges, prescriptions, emergency department visits, controlled-substance (e.g., narcotics) use and homecare.

The ICES Data Repository also holds data from other sources such as census information, social services, and immigration data. These non-health data may be collected and linked in certain limited circumstances with health data to provide a clearer picture of how other factors affect the population's health[12]. This additional information is critical to answering important

[9] *Freedom of Information and Protection of Privacy Act* [FIPPA], R.S.O. 1990, c. F.31

[10] *Privacy Act* (R.S.C., 1985, c. P-21)

[11] These may identify, either directly or by proxy, as any of those population groups.

[12] The ability for ICES to link health data to non-health data is limited, legislatively and contractually. The reasons underpinning these limitations is discussed at Part 3, section 3.

questions about the social determinants of health.[13] For example, an extract from a database of landed immigrants maintained by Immigration, Refugees and Citizenship Canada allows ICES to evaluate the particular health care needs of recent immigrants.

In 2017-18, ICES was involved in the creation of 492 peer-reviewed publications, and supported the research questions of over 30 unique knowledge users within the health system.[14]

Privacy and Security Practices and Procedures

As a PE, ICES is in a unique and privileged position to be able to collect individual-level data without consent from a variety of health stakeholders and a limited number of non-health stakeholders. In order to protect the privacy of individuals, and maintain strong research outcomes, the data managed by ICES is de-sensitized and coded. ICES de-sensitizes data by using a highly secure algorithm that replaces identifying information, such as names and health card numbers, with a confidential code for each record; the unique ICES identifier is entitled the 'IKN'. This identifier is created using a secure ICES algorithm that is based on the Ontario health card number. An IKN exists for every Ontario resident who has been eligible for health care over time. The IKN ensures the privacy and confidentiality of health information, while at the same time enabling it to be linked with other ICES data. Linking data from different sources allows researchers to understand how Ontarians interact with the healthy system from birth to death.

Only a restricted group of individuals from within ICES' Data Quality and Information Management department (DQIM) have permission to handle identifiable data for the purposes of de-sensitizing, creating the IKN and carrying out data quality and destruction procedures. These individuals are in a highly trusted position, receive special training and sign robust confidentiality agreements.

When a researcher requests access to the ICES Data Repository as part of an ICES project, the Privacy and Legal Office (PLO) conducts a Privacy Impact Assessment (PIA) to identify and minimize any privacy risks in the project, as well as to ensure that the request is permissible under PHIPA, ICES policies and procedures or any contractual obligations with data partners. These agreements with data partners may include certain parameters on the use, or re-use, of data collected by ICES. For example, in certain instances, additional permission from the original data collector who provided the data is required.[15]

Researchers are only able to access data after it has been de-sensitized, under gone a data quality assessment, and has been determined to be necessary for their specific project objectives. As set out above, any risks and recommendations are included in a PIA performed by the PLO and tracked to ensure that such risks are mitigated and recommendations addressed.

[13] The social determinants of health are the social and economic conditions that affect the overall health outcomes of individuals or groups.

[14] ICES, "Productivity and Impact Report 2017-2018" (October 2018) at 7.

[15] ICES, "Public Advisory Council Orientation Package" (February 2019) at 13.

Citizen Engagement

As part of ICES' Strategic Plan (2017-2020), in 2019, ICES created a Public Advisory Council (PAC). ICES recognized that as a steward of PHI, it needed to reflect the values of patients and the Ontario public more broadly. This includes establishing mechanisms to engage patients and the wider public in the design, delivery and dissemination of ICES research to increase transparency. Representing the voice of the public, the PAC will aim to provide guidance to ICES on what matters most to Ontarians in relation to research and analysis. Their thoughts, perspectives and values will help shape ICES research and influence the way data is used by ICES scientists to improve Health System Planning.[16]

[16] *ICES,* Ibid

Exploring the Health Data Trust Model

Background: Compute Ontario & ORION Smart Cities Governance Report

In November 2018, Compute Ontario (CO)[17] & ORION[18] submitted a proposal to the Ministry of Economic Development, Job Creation and Trade (MEDJCT) for the purpose of:[19]

(i) preparing a report focused on data governance and technological approaches to advancing Smart Cities, and
(ii) outlining a plan to explore the concept of a data trust model in collaboration with three organizations, through three demonstrable use cases.

As part of this initiative, CO and ORION tasked ICES to provide insights and explore the creation of a health data trust model that would allow a broader group of users to access PHI or data derived therefrom, while maintaining strong privacy and security protections, under the umbrella of a data governance framework. The section below sets out ICES' findings on the approaches and benefits of a conceptual health data trust.

Findings: ICES as a Health Data Trust

This section will achieve the following purpose: provide an overview of a legal data trust; explore the conceptual model proposed for ICES as a 'health data trust'; provide key considerations, and set out the advantages and disadvantages for the creation of a "health data trust" in Ontario.

I. Legal Trusts

The following is a general summary of relevant and significant principles of trust law in Ontario, and the manner in which they may be applicable to the specific circumstances of a data trust.

As described in more detail below, a trust is a tri-partite relationship involving:

[17] Incorporated in 2014 as a not-for profit organization and funded by the Ministry of Economic Development, Job Creation and Trade and has a pivotal role in the province's Advanced Research Computing and Big Data Strategy. https://computeontario.ca/

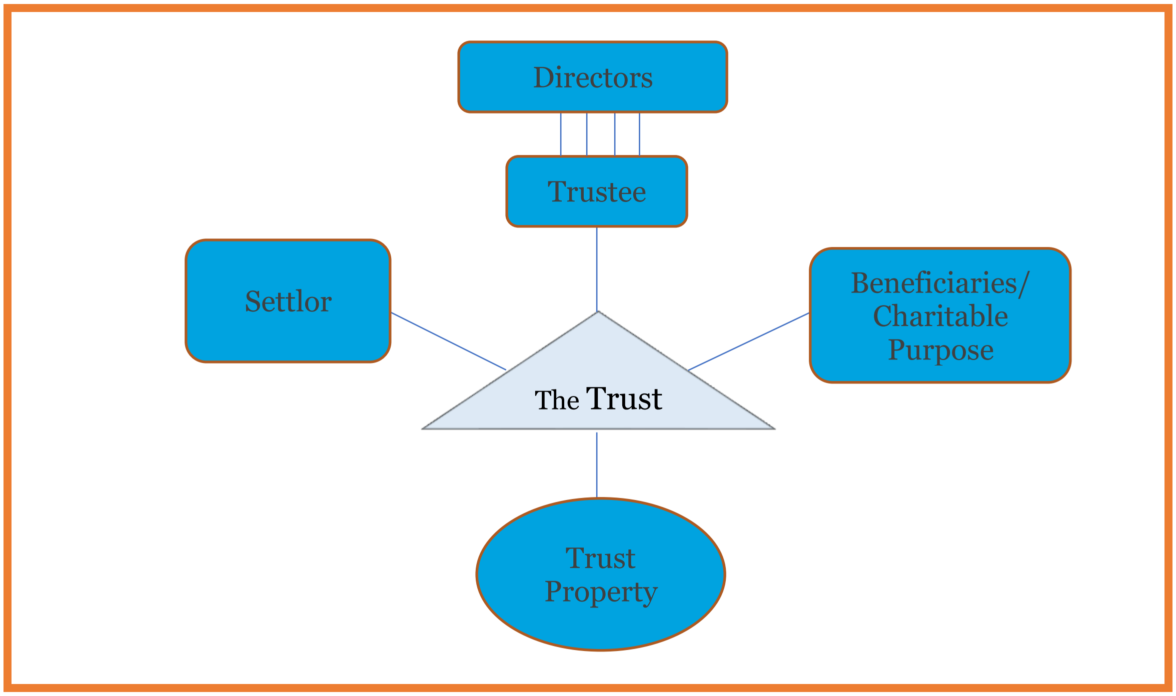
[18] ORION is a not-for-profit organization supporting Ontario's progress with essential digital infrastructure. https://www.orion.on.ca/

[19] Compute Ontario & Orion smart cities governance report submitted to: Ministry of Economic Development, Job Creation & Trade
November 13, 2018 (revised December 7, 2018).

- a settlor, who settles property on trust by transferring the legal and beneficial ownership of that property;
- a trustee, who acquires legal ownership of the trust property, and assumes a fiduciary obligation to administer the property for the benefit of one or more beneficiaries or purposes; and
- one or more beneficiaries or purposes. The beneficiaries are regarded as the equitable or beneficial owners of the trust property.

If the trustee is a corporation (such as ICES), then this tri-partite relationship can look like this:

Diagram #1: Trust / Tri-partite Relationship



The Settlor and Trust Property

The settlor determines the terms of the trust, which are documented in a trust instrument. That trust instrument identifies the persons (or purposes) that are to have the benefit of the trust property, and the manner in which they are to benefit. The settlor may act unilaterally in dictating the terms of the trust. Alternatively, the settlor may choose to negotiate those terms with the trustee so that the settlor can have confidence that the intended trustee will agree to act as trustee.

Although the settlor defines the terms of the trust (in consultation with the trustee, if desired) and settles the initial trust property, other persons may also contribute property to the trust (once the trust is established) if they wish to have that property dealt with as provided for in the trust instrument.

Key: For ICES, it may make sense for the settlor of the trust to be the entity that is the source of the bulk of the data that ICES administers

In most cases, the property held in the trust takes the form of money, securities or some form of tangible property. However, the law appears to recognize information and data as a form of property that can be held by one person on trust for the benefit of another.[20] Even so, the law in this regard is relatively undeveloped.

> **Key:** Although the law is undeveloped, there appears to be no legal obstacle to the settlement of trust with data as the trust property.

Beneficiaries / Charitable Purposes

Most trusts are established for the benefit of persons, but the law recognizes as valid, trusts that are established for identified purposes rather than persons. If those purposes are recognized as charitable then the trust may endure indefinitely, whereas if the purposes are not charitable, then the assets must be distributed within 21 years of the trust's settlement.[21]

The four legally recognized categories of charity are (1) the relief of poverty, (2) the advancement of religion, (3) the advancement of education, and (4) any other purposes beneficial to the community. Although case law has narrowed the potential breadth of this fourth category, the promotion or advancement of health and health care has been recognized as falling within this branch of charity.[22]

> **Key:** It is likely preferable for a data trust to be settled as a charitable trust established for the purpose of enhancing and improving the health of Ontarians.

Although it has been suggested that the beneficiaries might be the individual researchers who access and use the data, or the patients whose health would be improved by that research, there are two key problems with these proposals:

- Both groups of persons are too vague to be reasonably ascertainable; if so, such a trust will be invalid as it fails one of three requisite certainties, the certainty of "objects" to be benefitted by the trust. Indeed, it is arguable that the definitions are circular: for example, a researcher would presumably only become a "beneficiary" once the trustee determines to grant access to that person.

- Every beneficiary has standing to bring proceedings to enforce the terms of the trust, and also acquires certain other rights, such as a right to information about the administration of the trust property. Any trust with hundreds or thousands of beneficiaries may become administratively

[20] The leading case in this regard is *Phipps v. Boardman*, [1967] 2 A.C. 46 (H.L.), where the English House of Lords held that if information comes into the possession of a person in his or her capacity as a trustee, the information is effectively treated as type of trust property that can only be used by the trustee for the benefit of the trust's beneficiaries. *Phipps* was accepted on this point by the Ontario Court of Appeal in *R. v. Stewart* (1983), 42 O.R. (2d) 225. *Stewart* was reversed by the Supreme Court of Canada ([1988] 1 S.C.R. 963), which held that while information may be property for the purposes of the civil law; it was not to be regarded as property for the criminal offence of theft. The Supreme Court did not disagree that information could constitute property for certain civil law purposes.

[21] *Perpetuities Act*, R.S.O. 1990, c P.9, s. 16.

[22] See, *Alliance for Life v. Canada (Minister of National Revenue)*, [1999] 3 F.C. 504 (C.A.).

unwieldy for this reason. In contrast, a charitable trust is enforceable only by the Attorney General, and the Attorney General's agent, the Public Guardian and Trustee.

Key: there are obstacles to having individual researchers who access and use the data or the patients whose health would be improved by the research as beneficiaries

Trustees

Any one or more natural persons may act as the trustee(s) of a trust. There is no limit to the number of trustees, but having many trustees creates potential administrative problems – both because of the presumptive rule that trustees must act unanimously, and, even if the trust instrument varies this rule (for example, by providing for decision by simple majority or special majority), all trustees must participate before any decision can be taken.[23]

A corporation can also act as the trustee (or one of the trustees) of a trust. Although trust company legislation, both federally and provincially,[24] prohibits corporations from undertaking the "business" of a trust company unless registered as such under the legislation, this has generally be interpreted as applying only to corporations offering their services to the public. Thus, a corporation can act as a trustee without such registration so long as it does not offer to do so for members of the public.

Key: In the present case, ICES[25] would choose to serve as a corporate trustee of the proposed data trust, if the model were adopted.

i. Advantages and Disadvantages of the Data Trust Model

Although it is possible to create a data trust for the purposes of receiving, managing and sharing health care information and other information (e.g., social determinants of health), it is important to weigh the advantages to doing so against any disadvantages.

Advantages

Assuming the data trust is established as a charitable trust, then the trust may endure indefinitely. In addition, the charitable interests of the public (and by extension, the individuals whose data the trust is holding), could be safeguarded by the Attorney General, and the Attorney General's agent, the Public Guardian and Trustee, as well as the Canada Revenue Agency, both of which have oversight over charities operating in Ontario.

Aside from the legal accountability noted above, a trust may convey the notion of stewardship more so than other legal structures – namely, that the trustee of the trust has a special accountability to data sources and individuals whose data is held by the trust. Indeed, this perception appears to be the primary reason that certain entities are referred to as "data trusts".

However, could it be that an entity is not actually a legal trust, rather, the term "trust" is used to reflect the notional trust placed in the entity by participating agencies, and not to convey any

[23] This concept of a quorum—that is, a subgroup with legal authority to exercise the approval powers of the full group—is alien to a common law trust.

[24] *Loan and Trust Corporations Act*, R.S.O. 1990, c L.25, s. 213; *Trust and Loan Companies Act*, SC 1991, c 45, s. 412.

[25] ICES is a non-share capital corporation, registered as a charity, operating a research institute encompassing a community of research, data and clinical experts, and a secure and accessible array of Ontario's health-related data.

legal relationship? For example, Silicon Valley Regional Data Trust is not a legal trust. The project is based on the "trust" of the participating agencies that the use of the data is only to improve the outcomes for the children and youth whom they serve, and in no way to use data to harm a child. The "trust" is that all the participating agencies are using the access of data through the [Silicon Valley Regional Data Trust] to increase the equity and fairness for all children."

Furthermore, the trust relationship sought to be attained by a trust model is, in Canada, legally present for all corporations that are registered charities. The Public Guardian and Trustee and various courts have held that directors of a charitable corporation, like ICES, are trustees of the charitable property owned by the corporation.   This may render the perceived advantages of a data trust largely moot.

Key: Even though a trust may *convey* the notion of stewardship more so than other legal structures, the trust relationship sought to be attained by a trust model is, in Canada, already legally present for all corporations that are registered charities.

Disadvantages

The establishment and operation of a trust creates some administrative burdens. As an initial matter, it generally takes nine months or more to obtain charity status in Canada, from the date that the application is submitted. Considerable information would have to accompany the application. Thus at least one year should be allowed for this purpose.

The operation of a trust is foreign to many people and a data trust is a novel concept in Canada. Additional time, resources, as well as accounting, legal and governance resources, will have to be devoted to its ongoing operation.

The most significant disadvantage to establishing a data trust to receive, manage and share health care information and other information (e.g., data pertaining to the social determinants of health) is that it would not have any standing under Ontario's current public sector and health sector privacy laws to receive/collect that information. Specifically, it could not receive PHI from health care providers in accordance with PHIPA (absent individual consent), and would be no better placed than ICES in receiving non-health personal information from government entities.

In addition, a Health Data Trust in Ontario, under the present legal framework would be unable to receive de-identified data (derived from personal health information) from ICES for the purpose of further analysis or onward disclosures without REB approval.

Indeed, a recent report by Queen Mary University of London also concluded that 'trust law is not an appropriate legal structure for data trusts…the fundamental underlying concept, that those who are stewards of data should be responsible for proper oversight of its sharing and use, is achievable through different legal structures. Both an appropriate corporate structure and a contractual structure can be used to impose the required obligations on data stewards…[t]hese legal structures are more flexible and amenable to future development than the legal trust."[26] Further, one of the main problem areas is data protection and privacy law because "unless data sharing via a data trust was disclosed as a purpose and consented to when personal data were collected, sharing requires a fresh legal justification. Consent from data subjects would provide

[26] Queen Mary University of London "Data trusts: legal and governance considerations" (April 2019) at 8.

such a justification, but is challenging to obtain. Legitimate interest and performance of a public task are alternative justifications which might be available, but the scope of these is uncertain. Anonymisation and pseudonymisation do not necessarily solve this problem. If sharing personal data can be legally justified, the trust will of course need to implement processes to protect privacy and data protection rights, and to comply with data protection laws."[27]

These disadvantages render a data trust untenable for the proposed purpose unless it is linked to other MOHLTC action (i.e., the data trust is named as a health data institute) or regulatory change (i.e., the data trust is made a prescribed entity under PHIPA). In addition, other statutory amendments may be helpful. These additional actions or changes are described below.

Key: Trust disadvantages include –

1. It could not receive PHI from health care providers in accordance with PHIPA (absent individual consent), and would be no better placed than ICES in receiving non-health personal information from government entities.

2. Under the present legal framework it would be unable to receive de-identified data (derived from personal health information) from ICES for the purpose of further analysis or onward disclosures.

ii. Impediments in Privacy Statutes

At present, ICES is well-positioned to receive PHI and to a lesser degree PI.

- ICES is able to receive PHI from health care providers in its capacity as a PE under PHIPA.

- Because ICES is not a government institution for the purposes of the provincial public sector privacy law –– ICES is not *directly* restricted by FIPPA or MFIPPA in how it can collect other (non-health) personal information (however it may be restricted in other ways).

- Because ICES is a charity, it is not subject to the federal *Personal Information Protection and Electronic Documents Act*[28] ("**PIPEDA**") (which only applies to organizations engaged in commercial activity and is not applicable to charities).

The same considerations would apply to a charitable data trust if (like ICES) it was named in the regulations to PHIPA as a PE.

However, despite the ability to receive PHI and PI, ICES (and any other PE under PHIPA) is hampered in two respects.

[27] *Ibid.*

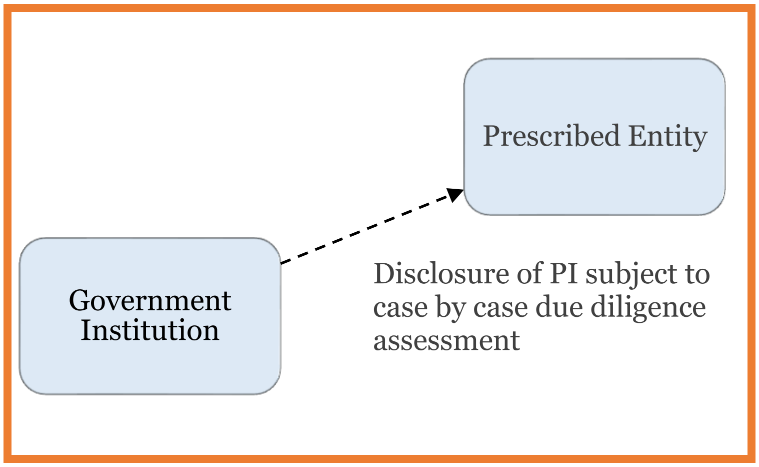
[28] *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5.

1. **Potential data sources are often restricted in their ability to readily disclose PI by privacy laws**.

Although ICES can receive PHI from health care providers (as a "PE" under PHIPA), provincial government entities and federal government entities are impeded in disclosing PI by FIPPA and the *Privacy Act*,[29] respectively. This means that each government entity will need to engage in a due diligence review of each disclosure, to assess the proposed disclosure against the entity's mandate and the purposes for which the information was collected (among other matters). Such case-by-case reviews can take time and resources to complete.

The same impediment would apply to a health data trust or any other entity seeking to serve as a data hub.

Diagram #2: Disclosure of PI to ICES proposes a challenge

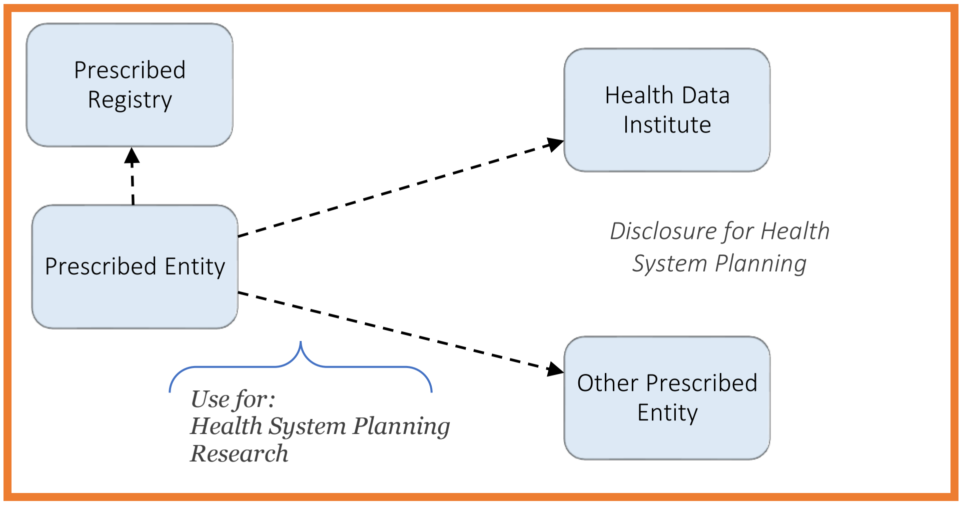

Prescribed Entity
Government Institution
Disclosure of PI subject to case by case due diligence assessment

2. **PHIPA restricts how PEs can use or disclose PHI (including non-health PI that is linked to PHI)**.[30]

Diagram #3: Current Use and Disclosure of Data

[29] *Privacy Act*, R.S.C., 1985, c. P-21.

[30] Under PHIPA, if non-health personal information (e.g., provided by a provincial agency) is combined with personal health information (e.g., provided by a healthcare provider under PHIPA), the resulting information is considered personal health information and subject to PHIPA's restrictions.



PHIPA only permits PEs to use or disclose PHI in limited ways – notably (among other grounds not relevant to this analysis):

- To use it for the purpose of analysis or compiling statistical information with respect to the management of, evaluation or monitoring of, the allocation of resources to or planning for all or part of the health system, including the delivery of services (collectively, "**Health System Planning**");[31]

- To use and disclose it for the purposes of PHIPA's research provisions as if it were a health information custodian (HIC);[32] and

- To disclose it to prescribed registries, to other prescribed entities for Health System Planning, or to a health data institute – in each case as if it were a health information custodian (HIC).[33]

PHIPA prohibits PEs from using or disclosing PHI for a purpose not expressly set out in PHIPA or its regulation.[34] As a result, this highly prescriptive regime casts doubt on whether any PE has the authority to de-identify (of its own accord) any PHI for onward disclosure to third parties (including to a data trust or other data hub) without REB approval.[35]

For example, if a research ethics board required PHI to be de-identified in order for it to be used for a particular research study, then ICES would de-identify that information prior to providing it to the researcher. It would do this as part of complying with PHIPA's research provisions. However, it is unclear whether ICES can, on its own initiative (*and not pursuant to a research ethics board approval condition*), de-identify PHI for the purposes of sharing it with third parties – whether for research or other purposes. This is a concern for the following reasons:

[31] *PHIPA,* Ibid. at s. 45(1).

[32] O. Reg. 329/04: General under PHIPA, at s. 18(3) and (4).

[33] O. Reg. 329/04: General under PHIPA, at s. 18(4).

[34] *PHIPA*, Ibid. at s. 45(6).

[35] De-identify means to remove the direct personal identifiers from data to reduce the risk that an individual can be identified.

- Under private sector privacy laws, such as PIPEDA, it is widely accepted that an organization is entitled to de-identify personal information under its control without needing the prior consent of individuals – even where this is not specifically set out in statute. Although the act of de-identification is a use of personal information, it is generally understood as a use that does not require consent. For public sector privacy laws, like FIPPA, similar arguments can be made.

- Unlike the private and public sector laws noted above, PHIPA includes a *specific* provision that permits a health information custodian to "use personal health information… in a manner consistent with Part II [of PHIPA], for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual".[36] [37]

- PHIPA does not expressly extend this de-identification provision to PEs.

- Applying common principles of statutory interpretation, if ICES is expressly permitted to do certain things that a HIC can do (i.e., analysis, research and engage in disclosures of personal health information for research), but not expressly permitted to do other things that a health information custodian can do (i.e., de-identify personal health information with a view to possible disclosure), then the legislature can be said to have intended this distinction. *On this basis, ICES may be unable to assert that it has the ability to de-identify personal health information separate from research ethics board approval conditions.*

[36] *PHIPA*, Ibid. at s. 37(1) (f).

[37] Although out of scope of this memorandum, presumably consistency with Part II of PHIPA requires a health information custodian to protect the personal health information pending de-identification, to effectively de-identify it, and to reference the purposes of the de-identification in the written public statement required by subsection 16(1) of PHIPA.

III. RECOMMENDATION

ICES as a Data Safe Haven

The purpose of the report is to explore how ICES could allow a broader group of users to access PHI or data derived therefrom, while maintaining strong privacy and security protections, under the umbrella of a data governance and ethics framework. To summarize, at present, ICES can already be considered a 'Data Safe Haven' due to its strong privacy and security protections and unique designation in PHIPA. Further, ICES does have some flexibility to allow certain users to access PHI. As set out above, ICES is able to do the following:

- Collect and use PHI from HICs without consent
- Use and disclose PHI for research only (with REB approval) as if it were a HIC
- Disclose PHI to the same HIC who provided it in the first place (as long as it does not contain any additional identifying information)
- Disclose PHI to prescribed registries and to other PE's –in each case as if it were a HIC for Health System Planning
- De-identify PHI for research purposes (with REB approval)

However, even though ICES is a Data Safe Haven there are legislative limitations that do not presently allow a *broader* group of users to access PHI or data derived therefrom. ICES is likely unable to disclose de-identified data (derived from health information) to a data trust or other legal entity for the purpose of further analysis or onward disclosures without REB approval unless ICES is named as a health data institute and/or there is regulatory change. The main reason is that it is unclear whether a PE has the authority to de-identify (of its own accord/initiative and not pursuant to a REB approval condition) any PHI for onward disclosure to third parties (including to a data trust or other legal entity).

Therefore, in order for ICES to further economic development as it relates to access to health data, some measure of regulatory/statutory amendment is required. A data trust will not, of itself, under the current legislative framework enable broader access to health data, particularly for economic development (i.e. granting access to private sector entities, including innovative start-up ventures). Indeed, the legal structure of an entity is not the answer; rather, some measure of MOHLTC and IPC action, change in regulation and/or statutory amendment is needed to address the impediments under privacy statutes, noted above.

Enabling broader access to data could involve one or more of the following options:

1. **Supporting the MOHLTC in designating ICES as an entity under PHIPA's health data institute provisions.**[38]

   Once created, the MOHLTC may direct HICs (including PEs, like ICES) to disclose PHI to that health data institute for Health System Planning purposes. Under PHIPA, a health data institute would then generate de-identified data for disclosure to the MOHLTC.

   PHIPA does not appear to restrict a health data institute from combining PHI from custodians with non-health PI from other sources prior to creating a de-identified data set for disclosure to the MOHLTC.

   While the MOHLTC is intended to be the recipient of this de-identified data, PHIPA does not prohibit the MOHLTC from engaging in onward disclosures of that data. Therefore, the MOHLTC could direct the institute to release de-identified data (on behalf of the MOHLTC) to third parties, such as researchers or others, to facilitate broader access and economic development activities, including innovation.

   However, there may be reluctance on the part of the MOHLTC or the IPC (who has an oversight role for health data institutes) to allow for wide-ranging disclosures of de-identified data, including to the private sector for commercial gain. Likely, the potential for such disclosure would need to be settled by the MOHLTC and IPC as part of creating the health data institute and finalizing its policies and procedures.

   It is important to note that the IPC's ongoing investigation in the creation, use and disclosure of de-identified patient data by electronic medical record companies may result in new guidance or restrictions on the creation of de-identified data from personal health information, and the disclosure of that data to private sector entities for analysis, research and development.

2. **Supporting amendments to PHIPA's regulations to include a provision which permits prescribed entities to de-identify personal health information for the purposes of onward disclosure to public or private sector entities – either as part of Health System Planning or research and development.**

   This would address the apparent restriction on the ability of ICES or any other prescribed entity to de-identify personal health information for onward disclosure.

   However, there may be reluctance in allowing research to occur without research ethics board approval (as would be required if the research involved personal health information). Similarly, as with the above option, there may be reluctance on the part of the MOHLTC to allow for wide-ranging disclosures of de-identified data, including to the private sector for commercial gain.

3. **Supporting amendments to FIPPA (or even MFIPPA) to facilitate the disclosure of PI by provincial government entities to ICES or ICES as a newly designated health data institute for Health System Planning or Research.**

   At present, ICES has been granted legislative authority to collect and use PHI without patient consent but currently there are no similar provisions in any legislative framework for

[38] *PHIPA*, Ibid. at s. 47.

ICES to collect and use non-health data without consent. Over the last decade, ICES has worked to build partnerships with organizations, including federal and provincial ministries, to acquire non-health data with the goal of examining the factors that impact health in a more comprehensive manner. If non-health data are not incorporated in policymaking, significant contributors to poor health will not be identified nor addressed. Partnerships with custodians of non-health data can take months in Ontario, if not, years because of the nuances in interpreting the legislative requirements for the disclosure of the personal information and the collection and use of such information. Since FIPPA governs the collection and use of PI from government institutions (including non-health identifiable data), amendments to FIPPA would facilitate the sharing of information without the need for case-by-case due diligence, and could be done through stream-lined data sharing agreement templates (similar to the way ICES engages with health data partners, HICs). It is posited that a similar case would exist for MFIPPA but this particular analysis has not yet been explored.

In conclusion, there are disadvantages to ICES as a Health Data Trust and therefore, it is proposed that with the appropriate legislative amendments, a more accurate term is ICES as a Data Safe Haven. The following specific amendments would likely allow disclosures and uses not limited to research and ensuring that municipalities and other levels of government could access data related to service delivery.

Suggestions include:

- ICES to be named as a health data institute in PHIPA regulations for onward disclosures to third-parties such as researchers or others, to facilitate broader access and economic development, including innovation
- FIPPA to be amended to clearly permit ICES to collect and use PI (non-health data) for wider system planning and evaluation (evidence-based policymaking)
- MFIPPA to be reviewed to assess whether ICES can collect and use PI (non-health) data for municipal system planning and evaluation (evidence-based policymaking) and if not, to amend accordingly
- PHIPA and FIPPA to be amended to enable a ministry disclosing PI to allow ICES to collect and link the PI with PHI, and disclose the linked dataset to third parties, whether they be academics, policy-makers, HICs, MOHLTC or other Ministries
- PHIPA and FIPPA (and possibly MFIPPA) to be amended to clearly permit ICES to de-identify PHI for the purposes of onward disclosure to third-parties as part of evidence based-policy making or other broader purposes set out by the government

Amendments such as the ones set out above, would allow for a Data Safe Haven such as ICES to provide broader access to PHI or de-identified data, and enable greater economic potential in Ontario. As a result, should there be support to enable broader access to ICES data it would be important to delineate a data governance and ethical use framework that would continue to ensure that ICES is entrusted with the data of Ontarians and build on principles such as transparency, data protection and ethics. The section that follows (Part 4) describes high level principles that would need to be included in an optimal data governance and ethical use of data framework that could be leveraged for this purpose of "Broader Access to Data."

Principles – Data Governance and Ethical Use Framework

In order for ICES as a Data Safe Haven to provide greater access of data, it is proposed that a data governance and ethical use framework for ICES would be useful. The following section describes the basis for a framework.

Introduction: The Need to Balance Data Protection, Ethics and Use

It is becoming a well-entrenched notion that recent waves in technological progress over the past decade as a result of digital capabilities are transforming society, including Ontario.[39] For example, a recent federal government white paper documented that according to IBM, 90 percent of the world's data has been created in the last two years.[40] The sheer power of digital and data processing and the volume of growing data are reshaping the global, federal, provincial and municipal economies. The power of this big data "has the potential to provide governments with greater insights into quality and effectiveness of services and programs such as healthcare, social services, public safety and transportation."[41] It is for this reason that an institution such as ICES which has been entrusted a steward of one of the largest data repositories in the province has the potential to provide the public sector and perhaps even the private sector with greater insights into the status of programs and services, and likely not just limited to healthcare.

As set out above, ICES currently has legislative limitations in respect of how it can use big data; at present it can only use or disclose data as a PE or for research purposes (with REB approval). Should legislation be amended and a model for greater access is adopted, a data governance and ethical use framework can be valuable to ensure that the ethical use of data is balanced with adequate data protection.

Moreover, such a framework must also be grounded in a modern approach to using data. There a number of frameworks that have been developed in recent years, such as for example, one developed by the Wellcome Trust that focuses primarily on the public attitudes towards public sector vs. commercial access to health data,[42] or another framework developed by researchers in the UK which focuses primarily on data access for research purposes.[43] There are elements from these frameworks that would be relevant to enabling broader access outside of research purposes or even outside of health data. Further review would need to take place to assess which

[39] Canada. Digital and Data Consultations, *Roundtable Address* (2018).

[40] IBM Marketing Cloud "10 Key Marketing Trends for 2017" Digital and Data Consultations Federal Government White Paper, (2018).

[41] Information and Privacy Commissioner of Ontario, "Big Data and Your Privacy Rights, Privacy Fact Sheet" (January 2017)

[42] Ipsos MORI for the Wellcome Trust "The One-Way Mirror: Public Attitudes to Commercial Access to Health Data" (March 2016) <https://www.ipsos.com/sites/default/files/publication/5200-03/sri-wellcome-trust-commercial-access-to-health-data.pdf>

[43] Tanvi Desani, Felix Ritchie & Richard Welpton, "Five Safes: Designing Data Access for Research" (2016) 1601 University of West of England Working Paper. <http://eprints.uwe.ac.uk/28124/1/1601.pdf>.

framework or which combination of principles would be important in a given data governance framework, but ultimately, in order to apply any framework and "fully maximize the innovation potential of digital and data technologies, a high level of trust, creativity, adoption and inclusion"[44] must be accepted by Ontarians. Therefore the social acceptance or 'social license' for use of the data is likely the primary driver for any data governance and ethical use of data framework.

The Driver: Social License

There is growing support for increasing the use of PHI to strengthen the health care system.[45] In particular, a recent survey of Canadians found that "more and more Canadians support the secondary use of information to monitor or evaluate the health care system; to anticipate and address public health issues; and to prevent improper uses of the health care system."[46] Further, the same study found that Canadians are similarly "increasingly comfortable with sharing their own health information across settings and for research. In fact, more than 75% of Canadians surveyed were comfortable with sharing their health information with other health organizations, with the health department in their province, with statistical organizations such as CIHI and Statistics Canada, and with health researchers." In addition, "support for health research increased from 80% to 88% of respondents if individuals were assured that their name and address would be removed." However, the one objection was that more than 80% of Canadians were not comfortable sharing their health information with private and for-profit organizations.[47]

Encouragingly, there is greater support for secondary use of health data for research purposes. Although the study did not ask respondents to comment on the use of data for evidence-based policy-making or any other such related purposes, the bigger issue appears to be the use of such data by the private sector. In fact, a recent Ontario study involving focus groups also found mixed and greater negative reactions to the use of data by the private sector.[48] It follows then, that in developing a data governance and ethical use framework, the use of the data by both the public and private sector must be clearly identified and transparent to ensure that an organization who is the steward of a data repository continues to be entrusted with the privilege.

Trust is therefore the "primary reason for [social] acceptance. Trust [can be] viewed as (1) a set of specific beliefs dealing with benevolence [the extent to which someone believes the use is for good], competence, integrity, and predictability; (2) the willingness of one party to depend on another in a risky situation [such as the collection and use of identifiable data]; or (3) the combination of these elements."[49] Trust is dynamic, must be earned and can easily be lost. In

[44] Bhaskar Chakrovorti, Ajay Bhalla & Ravi Shankar Chaturvedi, "The 4 Dimensions of Digital Trust, Chartered Across 42 Countries" (February 19, 2018), Harvard Business Review.

[45] Canada Health Infoway & Canadian Institute for Health Information, "Better Information for Improved Health: A Vision for Health System Use of Data in Canada" (June 2013).

[46] *Ibid.*

[47] *Ibid.*

[48] Alison Paprica, Magda Nunes de Melo & Michael J. Schull "Social License and the general public's attitudes toward research based on linked administrative health data: a qualitative study" (2019) 7.1 CMAJ Open.

[49] Keng Siau and Weiyu Wang, "Building Trust in Artificial Intelligence, Machine Learning, and Robotics" (March 2018) 31.2 Cutter Business Technology Journal, 47.

this instance, trust – "depends essentially on making good use of the data. This means using the data to generate benefits, refusing to use the data for purposes that might stigmatize or otherwise harm the population offering the data, and sharing the results openly with the data subjects."[50]

The diagram below illustrates different degrees of social license. If an institution such as ICES establishes credibility, the social license rises to acceptance and eventually to a level of approval. Over time, if trust is established and not lost, the social license could rise to the level of psychological identification, where the use of data is engrained as a fundamental component of society not easily rocked by socio-political forces.[51]

Diagram # 4: Trust Pyramid for a Social License to Operate (SLO)

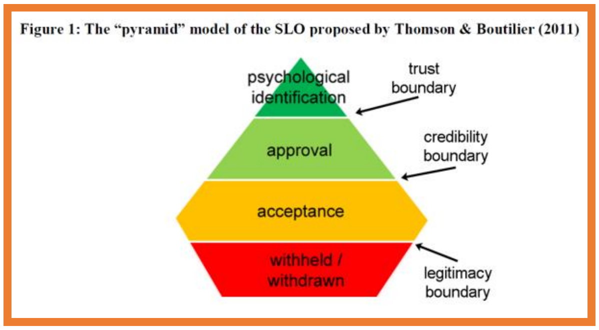


Figure 1: The "pyramid" model of the SLO proposed by Thomson & Boutilier (2011)

The following section explores at a high-level principle that may be incorporated in a data governance ethical use framework if ICES is named as a Data Safe Haven for Ontarians. Ultimately as set out above, these principles would need to be reviewed and further assessed before being formally incorporated in any framework.

Principles for Balancing Opportunities and Risks in a Data Governance and Ethical Use Framework

(i) Principle #1: Data Privacy

The Organization for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980)[52] articulated eight (8) basic principles of data protection (collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability). The OECD Principles form the basis of many privacy statutes in Western countries, including Canada and provincially in Ontario and indeed is the framework utilized in any privacy analysis currently employed by ICES as mandated by the IPC. In the future, regardless of whether

[50] Catherine Stinson, "Healthy Data: Policy solutions for Big Data and AI Innovation in Health" (December 2018), 179 Mowat Research at 18.

[51] Robert G. Boutilier & Ian Tomson "Modelling and Measuring the Social License to Operate: Fruits of a Dialogue Between Theory and Practice" (2011) Social Licence, 1-10.

[52] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* OECD Privacy Guidelines (2013).

Ontario continues to utilize the OECD framework or another framework to capture privacy risks, any framework must continue to ensure that Data Privacy is included.

(ii) Data Security

Billions of records containing personally identifiable information have been exposed globally.[53] Causes of data breaches have also evolved and include hacking, phishing and ransomware. These data breaches are simultaneously becoming more and more devastating and costly.[54] It is for this reason that Data Security is crucial to data protection.[55] Even though cyberattacks are growing, a recent study found that by offering transparency and enabling individuals to have insight and a level of control over their information, public perceptions of cyber breaches were tempered.[56] Effectively, research has found that "individuals do not punish breached firms that provided both transparency and control."[57]

Any data governance framework should take into account cybersecurity and security posture to guide decision-making related to data use.

(iii) Data Education

A framework may also take into consideration that not every population group has "data-friendly culture" or is "data-literate."[58] Digital Literacy is defined as "how people understand the data they work with or share, including how much they are aware of the positive and negative impacts of data use and sharing. Digital literacy includes both actors who are using the data and those whose data is being used." [59] A framework may include a review of whether the use of the data is ethically robust, criteria to evaluate could include (if relevant):

- what is the digital literacy of potential users of data;
- what is the digital literacy of the individuals who are comprised of, or are the source of the data? [60] ; and
- Is greater transparency required for this population group?

(iv) Data Empowerment

Internationally there is a citizen-driven movement aimed at defining the scope of ownership rights. The main question being considered is who owns the data that fuels our data-driven

[53] Ginger Zhe Jin, "Artificial Intelligence and Consumer Privacy"(December 18 2017) National Bureau of Economic Research Working Paper No. 24253.

[54] Teresa Scassa "Considerations for Canada's National Data Strategy" (2018), *Centre for International Governance Innovation,* online: < https://www.cigionline.org/articles/considerations-canadas-national-data-strategy>

[55] United Nations Development Group, *Privacy, Ethics and Protection Guidance Note on Big Data for Achievement of the 2030 Agenda,* UNSDG (2017) at 5.

[56] Kelley D. Martin, Abhishek Borah, Robert W. Palmatier, "A Strong Privacy Policy Can Save Your Company Millions" Harvard Business Review (February 15 2018)

[57] Harvard. Ibid.

[58] Muhammad Mamdani and Andreas Laupacis, "Laying the digital and analytical foundations for Canada's future health care system" (January 8 2018) 190.1 CMAJ

[59] United Nations Development Group, *Privacy, Ethics and Protection Guidance Note on Big Data for Achievement of the 2030 Agenda,* UNSDG (2017) at 5.

[60] UNDP Ibid. at 9.

society and what are the limits of any ownership rights?[61] In essence, is the data-relationship on the basis of data stewardship or data rights transfer? The scope of data ownership matters because if an individual owns the data that relates to them, it is undeniable that they retain a stake in that data, such as who can access and how the data is used.

The scope of data ownership rights is also being litigated in the courts.[62] Questions continue to include: rights of access to data, rights to own or control data and the public interest in relation to publically accessible data.

Furthermore, there is an "increasing desire among Canadians to access their medical records online."[63] A framework may also consider whether

- the use of the data enables individuals to access their own data; or
- the use of the data would lead to a complete loss of control by ICES; or
- the data use is in the public interest.

(v) Data Justice

With the rise of big data, commentators and experts are increasingly concerned that the data used to shape decision-making do not propagate social inequities in any data-driven processes. [64]

For example, during President Obama's presidency, the White House published a Report entitled 'Big data: Seizing Opportunities, Preserving Values.' The report found that "big data analytics have the potential to eclipse longstanding civil rights protections in how [personally identifiable information] is used in housing, credit, employment, health, education and the marketplace."[65] In addition, to those civil rights set out in the document, consider also how immigration, public safety, policing and justice system could be impacted as a result of algorithmic processing of big data.[66]

A framework must therefore consider the type of data and ensure that any use is ethically robust to guard against bias. In order to do so, it is opined that by denying access to or preventing retention of [data on race, ethnicity, gender and other sensitive attributes] will make it harder to detect and remedy bias and deny all segments of society the full potential of AI's benefits. But, at

[61] Considerations for Canada's National Data Strategy, Teresa Scassa (2018).

[62] Teresa Scassa "Considerations for Canada's National Data Strategy" (2018), online: Centre for International Governance Innovation < https://www.cigionline.org/articles/considerations-canadas-national-data-strategy>

[63] Canada Health Infoway, "Connecting Patients for Better Health: 2018" (2018), online: <https://www.infoway-inforoute.ca/en/component/edocman/resources/reports/benefits-evaluation/3564-connecting-patients-for-better-health-2018>

[64] Teresa Scassa "Considerations for Canada's National Data Strategy" (2018), online: Centre for International Governance Innovation < https://www.cigionline.org/articles/considerations-canadas-national-data-strategy>

[65] U.S., Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (May 2014) at 3.

[66] Jonathan Obar & Brenda McPhail, "Preventing Big Data Discrimination in Canada: Addressing Design, Consent and Sovereignty Challenges" (April 12, 2018) *Centre for International Governance Innovation,* online: < https://www.cigionline.org/articles/preventing-big-data-discrimination-canada-addressing-design-consent-and-sovereignty>

the same time, it is important to carefully control the availability and use of such data to ensure that it is not used to facilitate discrimination."[67]

Secondly, another important point that may need to be included in a framework is how to guard against predictive policymaking. It has been suggested that the generation of algorithms is, "undertaken by people and inevitably reflects the conscious and unconscious biases of those responsible for generating the data."[68] This can lead to biases even if those biases and mindsets were not intended.

Thirdly, another important item to be considered in a framework is whether vulnerable and marginalized people can access data. Even if all data are equal, not all people can access data equally.

Lastly, a data governance framework could also propose that because vulnerable communities are disproportionately susceptible to big data discrimination there should be an acknowledgement of the challenge of biased data sets[69] and the challenge of biased algorithms. Such acknowledgements could be included in publications if the use of the data is for research purposes or in reports if the data is used for broader public policy reasons. Ultimately there needs to be accountability and due consideration to the challenge of biases.

As one commentator suggested, let's "do it the 'Canadian way' – the pursuit of economic innovation within a framework of….data justice"[70]

(vi) Data Sovereignty

Data Sovereignty is the ability to control what (if any) data leaves Canada. A vast amount of data is stored or communicated outside our borders. [71]

At present, there does not appear to be any appetite to disclose PHI or PI outside of Canada. In fact, it has been suggested that due to "policy arbitration between nations … Canadian PHI should remain in Canada until international or bilateral rules are developed – we must look to domestic courts and lawmakers for restitution and enforcement."[72] But what about data that has been summarized or even de-identified? Should there be any consideration to the notion of data

[67]Centre for Information Policy Research at 18.
Jonathan Obar & Brenda McPhail, "Preventing Big Data Discrimination in Canada: Addressing Design, Consent and Sovereignty Challenges" (April 12, 2018) *Centre for International Governance Innovation,* online: < https://www.cigionline.org/articles/preventing-big-data-discrimination-canada-addressing-design-consent-and-sovereignty>

[68] Blayne Haggart, "The Government Role in Constructing the Data-Driven Economy" (2018) *Centre for International Governance Innovation,* online: <https://www.cigionline.org/articles/governments-role-constructing-data-driven-economy>

[69] Jonathan Obar, *ibid*.

[70] Lisa Austin "We must not treat data like a natural resource", *Globe and Mail* (July 9 2018), online: < https://www.theglobeandmail.com/opinion/article-we-must-not-treat-data-like-a-natural-resource/>

[71] Teresa Scassa "Considerations for Canada's National Data Strategy" (2018), *Centre for International Governance Innovation,* online: < https://www.cigionline.org/articles/considerations-canadas-national-data-strategy>

[72] Sachin Aggarwal "Treasure of the Commons: Global Leadership Through Health Data" (March 13, 2018), *Centre for International Governance Innovation,* online: <https://www.cigionline.org/articles/treasure-commons-global-leadership-through-health-data >

sovereignty for this type of data as well? A framework would provide an opportunity to assess whether:

- there is an ability to control data that leaves Canada;
- there are any compliance issues on the part of the data requester;
- there is a data privacy or data security strategy based on type of data; and
- there has been any due diligence on the third party data requester.

(vii) Oversight

Frameworks must be accompanied by strong accountability and oversight measures.[73] Oversight mechanisms may include committees or appropriate interaction with the enterprise risk management framework of an organization.

The overall goal is to govern data to manage risk, but continue to extract value from the data while protecting the public.[74] A framework should ultimately define responsibilities for how people manage and make a decision about data so that people are properly organized and make the right decision[75] - to foment an environment of transparency, trust, integrity, accountably.

Conclusion

These seven (7) principles are important for a framework as blanket consent is becoming more common,[76] "collecting data once and making it available as appropriate for secondary use [under a data governance model centered on a spectrum of ethical use of data] optimizes current processes, reduce duplication of effort, and leverage investments made in the public system."[77] However, as also stated above, there may be other principles that would need to be assessed and reviewed in a given data governance and ethical use framework. If ICES is provided with an opportunity to enable broader access to its Data Repository it would undergo an analysis to consider which framework is most suited to our role in the system.

Ultimately though, as stated by the *Declaration on Ethics and Data Protection in Artificial Intelligence, 40th International Conference of Data Protection and Privacy Commissioners* (Tuesday, October 23, 2018, Brussels) – "developing common governance principles in order that data use is in accordance with ethics, human values and respect of human dignity“ is central to the discussion on broader access to data.

[73] Privacy International and Article 19 (April 18) Privacy and Freedom of Expression in the Age of Artificial Intelligence

[74] Piyush Malik, "Governing Big Dial: principles and practices" (2013) 57(3/4) IBM Journal of Research and Development.

[75] David Plotkin, *Data Stewardship and Data Governance: How they fit together*. (Elsevier Inc., 2014).

[76] Catherine Stinson, "Healthy Data: Policy solutions for Big Data and AI Innovation in Health" (December 2018),

[77] Canada Health Infoway, "Better Information for Improved Health: A Vision for Health System Use of Data in Canada" (June 2013) at p.

Economic Potential

In the Managing Transformation: A Modernization Action Plan for Ontario produced by Ernst and Young LLP, a key recommendation for government and the broader public sector was "a relentless focus on data and analysis to strengthen the government's ability to drive greater efficiencies and better outcomes."[78] This report highlighted the siloed, often incomplete and low quality nature of the data currently used by government to evaluate its programs and policies. Therefore, multiple primary and secondary benefits can be realized with the development of a Data Safe Haven as described above that will:

(i) enable linkage and de-identification of health (PHI) and non-health (PI);
(ii) link data that is not centrally housed by a single data custodian (e.g., federal and provincial data); and
(iii)allow for access to a broad range of stakeholders and beneficiaries that have a public interest, beyond academic researchers, in accessing the data.

Allowing policy makers and health system stakeholders use actionable data to provide insights that will improve health policy will produce direct economic impact for municipalities and health teams through reduced health expenditure. The creation of a Data Safe Haven will have secondary benefits of driving economic development and job creation by feeding into the burgeoning innovation economy in Ontario. As noted above, public focus groups have expressed concerns over allowing private sector access to identifiable data. However, these concerns may be allayed with the management of such access by a trusted Data Safe Haven responsible for controlling access to data that is governed by Data Governance and Ethical Use of Data Committee with public and patient representation. The risk of negative implications of profit motive are mitigated by a committee that evaluates the project for public benefit.

In a recent OECD report on digital transformation and the economy, the authors opined "Understanding and acting on the economic and social dimensions of digital transformation is increasingly critical as the digital economy becomes the entire economy."[79] To succeed and realize the full economic and social benefit that lies before Ontario with its largely centralized health and social systems, mechanisms to bring these data together in a safe and secure manner, such as the Data Safe Haven need to be implemented. Results from the Federal Innovation, Science and Economic Development Canada public consultations on digital research infrastructure and national data pointed to three key elements to position Canada to lead in a data-driven economy:

(i) understanding the future of work [and workforce];
(ii) unleashing innovation; and
(iii)privacy and trust.

The report on the consultations highlights that these three are elements is "related and mutually-reinforcing."[80] We contend that a Data Safe Haven embodies these elements. With

[78] Ernst & Young LLP, "Managing Transformation: A Modernization Action Plan for Ontario". (September 2018).

[79] Organization for Economic Co-operation and Development, *Vectors of Digital Transformation*, 3, (November, 2017).

[80] Government of Canada, Discussion Paper "Positioning Canada to Lead in a Digital- and Data-driven Economy", <https://www.ic.gc.ca/eic/site/084.nsf/eng/00007.html>.

fairly straightforward changes to legislation and with only modest investment, ICES could serve as this Data Safe Haven providing a significant direct and indirect return on investment to Ontario and its municipalities.

A key recommendation going forward is for a relentless focus on data and analysis to strengthen the government's ability to drive greater efficiencies and better outcomes.

Appendix

Municipal Health Unit Use Case: Development of Test Bed Environment for Data Access

As noted in this report, under PHIPA a prescribed entity like ICES may only provide access to health data to third parties for a limited range of purposes. Although PHIPA permits a prescribed entity to use health data for evaluation, planning and monitoring of the health system, it does not allow a prescribed entity to release this data to health system stakeholders for these purposes. ICES cannot, for example, provide the health data that it has spent years collecting and integrating from multiple sources within the health sector to a hospital or LHIN to enable them to evaluate the effectiveness of its programs and services. Lacking access to the required data, these health system stakeholders are often forced to rely on ICES to evaluate their own programs and services on their behalf. In some cases, this is not optimal, particularly where health system stakeholders are able to carry out scientific analysis but merely lack the data that ICES holds. Having to rely on ICES lengthens the time for project completion, increases complexity, and in some cases drives up overall costs. This impacts health systems stakeholders' ability to conduct evaluations with efficiency and agility, which ultimately impacts patient outcomes and experience. In some cases stakeholders may choose to rely on ICES' scientific expertise to conduct the analysis; however it would be optimal for a choice to be provided.

In this use case, we sought to determine if municipal partners responsible for the delivery of health services and programs or the development of health policy could make use of the data resources available through a prescribed entity. This use case was developed in the following stages:

1) Identifying a health system stakeholder
2) Identifying questions feasible to be answered using the data under ICES' stewardship
3) Exploration of legal mechanisms by which a health system stakeholder could, for the purposes of the test case, obtain access to data to evaluate its own programs or services
4) Developing technical infrastructure enabling access to data
    a. Computational infrastructure
    b. Data infrastructure to reduce risk of re-identification
5) Future work

1) Identifying a health system stakeholder

Leveraging the Applied Health Research Question (AHRQ) process at ICES, where health system stakeholders may request that ICES perform analyses to inform public health policy, programs and services, ICES identified five municipal health system stakeholders that might benefit from direct access to ICES data. Initial consultation with these stakeholders identified that four of five stakeholders had personnel with the expertise to perform analyses on health administrative data. Of the four, one of the largest municipal health stakeholders – a public health department – was able to commit sufficient resources to this project. The public health department being Toronto Public Health, agreed to take part in this use case for accessing data to evaluate its core services.

2) Identifying feasible questions

ICES and Toronto Public Health (TPH) held several consultations to identify use case projects in which data from the ICES repository, if accessible to TPH staff, could be used to answer questions relevant to the daily operations of the health department.

Initial discussions focused on projects that would require linking data currently held at TPH with the ICES data repository to answer questions around the health of marginalized populations. While technically feasible, the anticipated timeline associated with importing health department data to ICES, processing and making that data "evaluation-ready" and establishing the requisite data sharing agreement was determined too long for the purposes of the test case project. Nevertheless, this indicates a future potential project and, more broadly, the importance of streamlining mechanisms for importation and linkage of data to provincial repositories, in developing truly smart cities.

Further consultation resulted in the following data elements and degree of importance for TPH (see Table 1).

Table 1. *Results from stakeholder consultations with Toronto Public Health identified data elements that would be of value if accessed in real-time by public health staff in a data safe haven.*

Indicators/Datasets	Importance to Public Health Surveillance	Rationale
Incidence and prevalence of Ischemic Heart Disease (IHD)	High	• Ischemic heart disease is a leading cause of death in Toronto for both sexes • IHD is linked to many modifiable risk factors • Related to cannabis health outcomes surveillance
Incidence and prevalence of Chronic Obstructive Pulmonary Disease (COPD)	High	• COPD is linked to public health interventions on smoking • COPD is related to cannabis health outcomes surveillance
Incidence and prevalence of Diabetes	High	• Diabetes is linked to public health interventions and many modifiable risk factors • Considerable variation by social determinants makes programs appropriate for data-informed targeted approaches
Incidence and prevalence of various psychiatric disorders (schizophrenia,	High	• No epidemiological data on psychiatric disorders while interest among internal partners is growing (e.g., Mayor Symposium on Mental health in 2018)

depression, anxiety)		• Related to cannabis health outcomes surveillance
Country of Origin and year of immigration, (Immigration, Refugees, and Citizenship Canada data)	High	• Data on immigration status may be related to chronic disease development (incidence) and prevalence • These data may inform targeted intervention strategies at the local level
First contact in the emergency department for mental health and addictions	Medium	• Indicates loss of opportunity for adequate outpatient and community-based care • May help with identifying communities needing help with accessing mental health resources before critical incidents
Repeat unscheduled emergency department visits	Low	• Might indicate issues with transition of care • Lower locus of control for public health staff
Rate of inpatient readmissions within 30 days of discharge	Low	• Might indicate issues with transition of care • Lower locus of control for public health staff

3) Exploration of legal mechanisms by which a health system stakeholder could, for the purposes of the test case project, obtain access to health data at ICES

Central to a smart city is the ability of municipal entities to have efficient access to health data from across the health sector. As mentioned in this report and the pre-amble to this section,

PHIPA does not allow a prescribed entity to provide direct access to the health data it compiles to third parties to enable them to evaluate the effectiveness of their own health programs and services (this report recommends legislative changes that could address this limitation).

To test our use case (i.e., whether direct access to provincial health data would enhance municipal decision making), the ICES Privacy and Legal Office undertook an assessment to determine that ICES is able to designate a TPH staff member (e.g., data analyst) as an agent of ICES for the purposes of completing the test case project, and by doing so, the health department employee would be legally authorized to access ICES' health data directly as if it were ICES doing so. The health department employee, as an agent of ICES, would be required to complete, at a minimum, privacy and security training and sign an agency and confidentiality agreement. The test case project would also be subject to a privacy impact assessment conducted by the ICES Privacy and Legal Office prior to commencement.

4) Developing technical infrastructure enabling access to data

a) Computational infrastructure

Leveraging ICES' ICES Data Analysis Virtual Environment (IDAVE) and the Ontario Data Safe Haven (ODSH), the ICES information and technology department has created a virtually moated environment in which ICES agents, such as an analyst from TPH, could remotely perform analytics on highly de-sensitized, individual-level data where the risk of being able to identify any person is extremely low. These data would be in the form of a dataset bespoke to the requirements of TPH. These data would be segregated from the ICES data repository and the ICES agent would only have access to the data required for the project.

Remote access would require two-factor authentication and the environment would be virtually moated such that data or analytic results cannot be removed from or printed from the IDAVE environment.

b) Data infrastructure to reduce risk of re-identification

Leveraging ICES' processes for remote access for third party researchers, ICES has developed and refined processes to allow a variety of authorized ICES agents, researchers, and health system stakeholders (the latter provided changes to legislation can be achieved) access to data that is highly de-sensitized. This infrastructure is able to assess data and determine the re-identification risk based on additional inputs (e.g., the qualifications of the analyst accessing the data). Data that do not meet appropriate risk thresholds will be further de-sensitized until the acceptable threshold for data release is met.

5) Future work

Future work will focus in two primary areas:

a) Operationalization of ICES-TPH collaboration in the Ontario Data Safe Haven (ODSH)

- An ICES staff scientist has been appointed to work with health department staff to identify a single question or issue to be addressed through access to data in the Ontario Data Safe Haven
- ICES staff scientist and ICES analysts will develop a dataset from the ICES data repository with the required elements to perform analytics to inform the issue
- ICES Privacy and Legal Office will develop agreements with the health department to allow a municipal staff member (analyst) to remotely access a highly de-sensitized copy of the data as an ICES agent – (for the purposes of demonstration in this project)
- Following completion of the previous steps, ICES will provide access to the highly de-sensitized data in a virtually moated environment (e.g., ODSH)

b) Modernization of Provincial Legislation

- ICES Privacy and Legal Office will detail amendments to current legislation (e.g., PHIPA, FIPPA, MFIPPA) that would allow for broader authorized access to qualified health system stakeholders working in the interest of Ontarians.

Compute Ontario

ICES

ORION