PHIPA Modernization Consultation

2004 to 2024: Toward a Data-Driven Health System

February 2023

Table of Contents

ABOUT ICES

ICES is an analytics and research institute that leverages population data to generate meaningful insights to improve policy, health care, and health outcomes. ICES is a not-for-profit corporation and registered charity formed in 1992. ICES is governed by a Board of Directors and guided by a Scientific Advisory Committee and a Public Advisory Council, both of which consist of members from diverse regions and communities across Ontario.

ICES' Mission is translating data into trusted evidence that makes policy and health care better and people healthier. To achieve this Mission, ICES collaborates with data custodians, government, policymakers, health system stakeholders, Ontario's Information and Privacy Commissioner ("**IPC**"), members of the public, First Nations, Inuit and Métis organizations, and communities to advance its Vision of improved health and health care for everyone through world-leading analytics and research.

Over the past 30 years, ICES has developed eight health research and analytic programs across a network of seven sites in the province, and a secure remote virtual access platform. ICES maintains a broad and diverse array of data and data environments that require a robust approach to privacy and security governance. ICES is unique in the breadth of its data, tools, and resources to support analytics, its ability to import and link data, and its capacity to support significant analytic activity (>400 new projects per year) and knowledge generation (>700 publications and related products per year).

ACKNOWLEDGEMENTS

Authors (Alphabetical order):
Rosario Cartagena, Chief Privacy and Legal Officer
Ash-Lei Lewandowski, Legal Counsel
Mike Paterson, (Acting) Chief Science Officer
Michael Schull, CEO
Todd Smeed, Director, Cybersecurity
Michael Smith, Director, Privacy & Legal Office
Marian Vermeulen, Sr. Director, Research, Data & Financial Services

Contributions by (Alphabetical order):
Mahmoud Azimaee, Director, Data Quality Information Management / Kathy Li, Manager, Privacy /Charles Victor, Sr. Director, Strategic Partnerships & Digital Services

INTRODUCTION

In the 20 years since Ontario's *Personal Health Information Protection Act*, 2004 ("***PHIPA***") was enacted, Ontario's health system has undergone fundamental shifts in its delivery of care, particularly through the increased integration of health services and a proliferation of health technologies that produce masses of digital health data. These shifts are evident in the new and expanding types of health care models, providers and services offered across the province. At the same time, there is a growing focus on advancing health equity and better understanding the social determinants of health, each of which carries implications for the scope and nature of the data required to evaluate and understand the health of individuals and communities.

Given that a modern health care system must be horizontally integrated across providers and organizations, it follows that an accurate portrait of a patient's care journey can be achieved only through seamless and real-time data sharing across an integrated care continuum. Similar seamlessness with data sharing is needed at the system and population levels to provide timely and accurate analytics and research on the health system itself. Fully realizing the benefits to patients, the public and the health system will depend on data for health care planning and decision-making purposes, such that any modernization efforts to *PHIPA* requires support for a robust analytics and research framework that can anticipate and authorize the necessary conditions for these changes. To maintain trust in the health care system, such a framework must also continue to maintain the privacy and confidentiality of the individuals whose personal health information is collected, used, and disclosed across the province.

ICES' submission is organized by carefully considering how best to achieve a learning health system by optimizing the valuable resource we steward – data – to best facilitate *PHIPA* modernization. We believe that modernization of the legislative, regulatory and oversight regimes that govern the use of health-related data is essential to achieving this learning health system. For the purposes of advancing the dialogue on *PHIPA* modernization, our commentary focuses primarily on the statute, but we have also included feedback on the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* (the "**IPC Manual**"). While the IPC Manual is not the subject of these consultations, ICES' ability to carry out its analytics and research permitted under *PHIPA* is directly linked to the IPC approving our practices and procedures pursuant to subsection 45 (4) of *PHIPA*, and is therefore contingent on compliance with the IPC Manual.

We have organized our written submission as follows:

a) Overview of why the Prescribed Entity role should be expanded;
b) Support for a privacy and security model that supports analytics and research;
c) Proposed statutory amendments to align with a modern health system; and
d) Proposed high-level revisions to the IPC Manual to enable these recommendations, while keeping privacy and security at the forefront of our operations.

The following is ICES' written submission to the Ontario Ministry of Health ("**MOH**").

---

1. Expanding the Role of the Prescribed Entity

Our perspective is primarily from that of a Prescribed Entity ("**PE**"). In our view, making better use of health data requires enabling PEs to take on an expanded role in *PHIPA*. Indeed, when *PHIPA* was first enacted, the foresight to include the designation of a PE was very novel and unique, and enabled Ontario to be an international exemplar for health data stewardship. 20 years later, it is apparent that the model of reputable institutions being able to conduct analytics to support provincial policymaking has been as asset to the government and health system stakeholders. The strengths of the PE model in Ontario include:

- Population-based analytics through statutory permission to access, link and analyze health data, with the goal of generating evidence and informing decision-making;
- Data Holdings curated by subject-matter experts;
- Strong oversight by a provincial regulator;
- Data stewardship trusted by data providers and the public through operational transparency and accountability; and
- With ICES specifically, an independent, not-for-profit institute that is arms-length from government and has used its status as a trusted data steward to forge important partnerships with partners, such as First Nations, Inuit, and Métis communities.

Notably, to conduct accurate population-based analytics, a PE's strength in supporting the government and health system stakeholders is predicated on a "no-consent" model. In other words, it is not possible to exist as a PE and understand the trends in population health if individuals must consent-in, or are able to opt-out of participating. In recognizing the historical misuse of data related to certain groups and communities, however, it is incumbent upon PEs to engage with the public, patients, and equity-deserving communities in the ways in which we work with data and undertake research and interpretation of any data analytics and findings. For example, ICES has created a Public Advisory Council to help guide its analytics and research to be reflective of Ontario's diverse communities; worked with First Nations organizations to

develop specific data governance models that are based on Indigenous Data Sovereignty principles; and is developing a race and ethnicity data framework in alignment with the communities the data represent.

Despite these strengths, there are challenges in complying with the IPC Manual while also operationalizing the effective provision of analytic and research services to Ontario stakeholders. In particular, the needs, expectations, and opportunities for the use of health data by PEs to improve health care, policy and outcomes have grown, yet the legislative framework has not similarly evolved.

2. ICES' Privacy and Security Accountability and Operating Models

For 30 years, ICES has and continues to be a credible, trusted and arms-length institution advancing the use of health data to provide answers to complex questions facing the Ontario government and its health system. Over these years, ICES has delivered high-value analytic and research services to key stakeholders, including researchers, Indigenous communities, health system partners and the government, and we have evolved our practices in ways to meet evolving demands while always remaining compliant with our regulatory regime. To remain relevant and responsive, our operational models need to be agile and adaptable over time. Increasingly, such responsiveness is challenged by legislative constraints enshrined in *PHIPA* some 20 years ago. For example, the combination of a high volume of unique projects and the complex legislative analyses required for such projects means that ICES' privacy assessments for new data collections can often take weeks to complete. We have included a description of our privacy work and our resources in Appendix "**A**". It is our view that *PHIPA* modernization affords an opportunity to remove statutory barriers complicating our analyses while maintaining IPC oversight to ensure accountability, transparency, and trust.

To best respond to these challenges, then, we have set out proposed statutory amendments to *PHIPA* that focus on improving the health system in privacy- and security-preserving ways. Further, in aligning our submission with the Ontario Health Data Council report,[1] which states that "Ontario must immediately take a common use, case-based approach to addressing the purpose-driven data needs at all levels of the health system," we have also included use cases to provide real-world examples of how purpose-driven uses of health data can drive better outcomes for all.

---

[1] *Ontario Health Data Council Report: A Vision for Ontario's Health Data Ecosystem*, online: Ontario.ca <https://www.ontario.ca/page/ontario-health-data-council-report-vision-ontarios-health-data-ecosystem>.

3. Opportunities for Statutory modernization

To best respond to the MOH's goals for health care delivery in Ontario, we have linked key government objectives to strategies for data use and proposed statutory revisions to *PHIPA* that would most effectively support these goals. As leaders in data analysis, PEs are an asset in Ontario and are indispensable partners in assisting government with solving challenges in the following five areas:

i. Creating the integrated health care system of the future;
ii. Achieving a stronger focus on health equity;
iii. Enabling cost-savings, efficiency and better outcomes in the health care system;
iv. Strengthening pan-Canadian analytics by leveraging extra-provincial data for health care planning; and
v. Adopting new technologies to optimize the health system.

Each of these key themes is expanded on below.

THEME	a) ALIGNMENT WITH THE INTEGRATED HEALTH SYSTEM OF THE FUTURE
Health System Goal	An integrated health system where patients can transition seamlessly between hospitals, physicians, Ontario Health Teams ("**OHTs**"), allied health professionals and community organizations.
Data Goal to Support Health System Goal	Data from multiple providers are used to support an integrated health system by expanding a PE's authorities for data sharing. Data from multiple providers collected by PEs enables the conduct of population-based analytics on an integrated health system for health planning, delivery and quality improvement initiatives, e.g., sharing personal health information ("**PHI**") on emergency room readmissions across custodians.
Current Legislative Barriers	PEs are very limited in their ability to disclose PHI. The collection and use authorities set out in section 45 of *PHIPA* enable PEs to be uniquely situated in Ontario in their possession of comprehensive, end-to-end individual- and population-level data. *PHIPA*'s disclosure limitations on most PEs, however, translate into barriers for using data to support an integrated health care system. PEs currently cannot complement capabilities and capacity of internal Ministry data, use its analytic and research functions, for example, to support OHTs in understanding patient populations, to track health care utilization or to monitor patient-level outcomes. Currently, most PEs are authorized to disclose PHI only to the following persons or in the following circumstances: • to a prescribed person, a researcher, another PE, or a health data institute; • to the health information custodian ("**HIC**") that originally disclosed the data, as long as the data does not include additional identifying information; • to a governmental institution where permitted or required by law, treaty, agreement or arrangement; • to the MOH or its designate for the purpose of an "electronic master person index"; and • to the MOH, upon its request, for COVID-19-related purposes. A key implication of these limitations is that many PE disclosures effectively become "research by default," meaning the purpose of the disclosure is required to be captured as research-related even in instances where the purpose of the disclosure and subsequent use is not research per se. This in turn creates additional time and resources spent on research ethics board ("**REB**") reviews for non-research purposes.
Proposed *PHIPA* Amendments to Realize Health System Goal	Amend *PHIPA* to authorize additional disclosure scenarios for PEs. Broadening the scope of scenarios in which PEs could disclose PHI could result in both cost- and life-saving benefits for the province. Disclosures of PE data could complement internal MOH data while supporting other HICs in determining and understanding patient populations, tracking health care utilization and monitoring health outcomes. **Specific legislative revisions:** • Permit a PE to disclose PHI as though it were a HIC for the purpose of section 38 of *PHIPA*. This would enable disclosure of ICES' comprehensive data to additional HICs for the purpose of timely health care. Recipients could include the MOH, hospitals, clinics, physicians, OHTs, etc. A HIC would be able to receive linked PHI from a PE customized to support unique, evidence-

	based health care delivery needs, as well as for improved quality, safety and cost-effectiveness purposes. • Permit a PE to disclose PHI for the purpose of section 40 of *PHIPA*. This would enable ICES to use its data to contact HICs or individuals where such individuals are at a significant risk of serious bodily harm, say through an increased risk of disease that ICES is able to determine through the linking together of its data, and of which the originally disclosing HIC and/or the individual otherwise would be unaware.
Use Cases	***MyPractice* Reports** ICES currently provides cuts of de-identified data to Health Quality Ontario to generate *MyPractice* reports. These reports provide physicians with data about their practices with an eye toward quality improvement. One of the key features of these reports is data about a physician's opioid prescribing habits compared with other physicians in the province. Because PEs are unable to disclose PHI to HICs (with the limited exception of disclosing back to the original HIC without any additional identifying information), *MyPractice* reports are limited to aggregate data that fall within a range (e.g., a percentage of patients prescribed a daily high dose of opioids) or are missing altogether due to the required suppression of small cells. So, for example, a report might show that a percentage of a physician's patients are receiving more opioids than what the physician is prescribing, meaning these patients are receiving opioids from additional physicians. But without knowing who these patients are, the physician is unable to adjust their prescribing patterns to improve their provision of health care. A revision to *PHIPA* that would permit a PE to disclose PHI as if it were a HIC for the purpose of section 38 would enable ICES to provide identifiable data in support of *MyPractice* reports, enabling physicians to better tailor their care to specific patients, which in turn would more effectively contribute to the quality improvement that is the basis of these reports. Since any PHI that includes additional identifying information would be limited to a physician's own patients, the disclosure of such PHI would be back to those within a patient's "circle of care" and would be limited to purposes directly related to improving health care delivery. **Hypothetical use cases that would benefit the health care system** • Using its scientific expertise, ICES could disclose highly curated PHI to HICs for service delivery or evaluation, planning and monitoring of the health system. It could also disclose PHI directly to individuals where identification of illness or disease is possible only through linkage of ICES data, and direct disclosure to an individual could prevent further illness or death. For example, ICES analytics could identify individuals who require follow-up care from their physicians, who may be candidates for specialty care or clinical trials, or for disease screening interventions.

THEME	b) A STRONGER FOCUS ON HEALTH EQUITY
Health System Goal	A health system that is more patient-centred and recognizes that health outcomes are not due solely to clinical or biological factors but are also driven by social determinants.
Data Goal to Support Health System Goal	PHI and Personal Information ("**PI**") can be easily shared by leveraging *PHIPA*, the *Freedom of Information and Protection of Privacy Act* ("***FIPPA***") and other relevant statutes. PEs easily collect, use and link PI with PHI to create valuable insights for health planning while improving health equity.
Current Legislative Barriers	It is very challenging for PEs to collect, use and disclose PI, and to link PI with PHI. Advancing health equity through consideration of the social determinants of health requires a recognition in health care legislation that health issues and outcomes are strongly affected by contexts and circumstances that exist outside of HICs and other clinical settings. Certain non-health data factors, such as an individual's race, ethnicity or socioeconomic status, may have a major impact on health care access, service delivery and outcomes. Note that even with the recent addition of Part III.1 of *FIPPA*, which sets out data integration and the formulation of "Extra-Ministerial Data Integration Units" ("**EMDIUs**"), there are still opportunities to better align *PHIPA* to ensure seamless analyses under both *PHIPA* and *FIPPA*'s legislative frameworks.
Proposed *PHIPA* Amendments to Realize Health System Goal	Amend *PHIPA* to help facilitate the collection, use and disclosure of health-related PI. *PHIPA*'s "mixed records" approach sets out that PHI includes information that is not PHI but that is contained in a record that includes PHI. It seems reasonable to extend this logic such that, if information that meets the definition of PI under another Act consists of information related to individual- or population-level health, or the wider social determinants of health, and the purpose of a collection of such data by a PE is to evaluate, plan or manage the overall health of the province and its health system, then such collection could be authorized as a collection of PHI, regardless of how the information is treated by the disclosing party. **Specific legislative revisions**: • Revise section 1 (Purposes) to include health analytics and research as express purposes; • Revise section 4 (Personal health information) to expand the definition of PHI to include information relevant to social determinants of health, as long as a collection, use or disclosure of such PHI is for health-related purposes, in order to limit unjustified use of potentially sensitive data; • Revise section 7 (Application of Act) to expand the application of *PHIPA* to expressly include PEs and researchers; • Revise section 45 (Disclosure for planning and management of health system) to include other organizations and persons who can act as if they were a HIC for the purpose of a disclosure to a PE, including where the information being disclosed consists of social determinants of health, and the PE is collecting the information to link the data with other PHI.

Use Cases	**Early Development Instrument ("EDI") Data** EDI is an educational tool created by the Offord Centre for Child Studies at McMaster University. It measures a child's ability to meet developmental expectations in areas of physical health and wellbeing; social competence; emotional maturity; language and cognitive development; and communication skills and general knowledge. Understanding the developmental health of children enables policymakers and researchers to create programs responsive to, and to better understand, children's needs. Developmental needs of children can be a direct, prior effect of social determinants of health while also directly impacting future health profiles and needs. Currently, the collection and use of EDI and similar data by PEs is very challenging because these types of data are commonly understood to be PI rather than PHI. In such cases, however, the PI is clearly related to individual- and community-level health, and a collection of EDI data by ICES would be for strictly health-related purposes. Nevertheless, there are neither clear collection nor disclosure authorities to enable use of EDI data for this critical work. Revisions to *PHIPA* that would enable a PE to collect EDI data as a subset of PHI could benefit the health care system by helping to identify the needs of children within specific communities to better evaluate and plan for appropriate health-related policies. Analytics and research using EDI data could answer important questions about social determinants of health and their interplay with other health-related factors affecting wellbeing and development. **Hypothetical use cases that would benefit the health care system** • An ability to collect Ontario Works ("**OW**") data from the Ministry of Children, Community and Social Services ("**MCCSS**"), and to link the data with PHI for analytics and research purposes would enable ICES data to be used to better plan for interventions such as structured psychotherapy for OW recipients with mood or anxiety issues. These analytics could determine how many OW clients are affected, what kinds of mental health services are already being provided, and other health outcome data. • Similar MCCSS data could be used to advise MOH on public health home visits among those receiving social assistance to better identify targeted care and cost savings. • PI linked with PHI could allow ICES to provide MOH with data in support of policy development around vulnerable populations, such as structured psychotherapy programs aimed at reducing the need for social assistance, or whether there are OHTs with large populations of vulnerable individuals and how these populations could impact an OHT's service provision. • An ability to collect data on Crown wards or others involved with Children's Aid Society, and to link the data with PHI for analytics and research purposes would enable ICES to provide MOH with data on long-term mental health outcomes, suicides, early deaths, etc. • A broad ability to link information commonly considered to be PI with PHI would enable ICES to provide broader access to data across multiple sectors to enable a strong, innovative economy that provides jobs and prosperity to Ontarians.

THEME	c) EARLY IDENTIFICATION OF AT-RISK INDIVIDUALS FOR PREVENTIVE CARE OR TREATMENT TO IMPROVE OUTCOMES AND REDUCE COSTS TO THE HEALTH CARE SYSTEM
Health System Goal	Prevention and/or early diagnoses of illness to offer and deliver earlier care to improve outcomes, and reduce costs and pressure on the health care system.
Data Goal to Support Health System Goal	Data collected through patient contact studies can support early identification of individuals at risk of, or suffering from, illness, thereby enabling providers to offer earlier initiations of prevention and treatment strategies. PEs conduct analytics at a population level to enable early identification of individuals who are at risk for research involving these individuals.
Current Legislative Barriers	Data collected by PEs cannot be easily used to support research that involves patient contact. Subsection 18 (4) of Ontario Regulation 329/04 (the "***PHIPA Regulation***") permits PEs to act as if they were a HIC for the purpose of section 44 of *PHIPA*. There is considerable interest in scientific communities to have PEs identify specific cohorts of individuals based on inclusion and exclusion criteria so that the individuals can be invited to participate in research. Under subsection 44 (6)(e) of *PHIPA*, however, a researcher cannot contact an individual, directly or indirectly, unless the HIC (in this scenario, the PE acting as if it were a HIC) first obtains the individual's consent to be contacted. For ICES, section 44 (6)(e) of *PHIPA* includes the following challenges: • ICES is not a known organization to many in Ontario, meaning it is inappropriate to contact individuals unexpectedly about their health. These individuals may feel that their privacy rights have been violated, which then risks reputational harm to ICES. • ICES is not operationally set up to engage in direct patient contact, which means any ICES involvement in patient contact can lead to project delays. • Including ICES in patient contact initiatives can increase research costs.
Proposed *PHIPA* Amendments to Realize Health System Goal	Revise section 44 (6)(e) so that a PE acting as if it were a HIC is not required to obtain the individual's consent to being contacted before a researcher, to whom the PE discloses PHI, contacts the individual. **Specific legislative revisions** (proposed additional language is underlined): ***Disclosure for Research*** (6) A researcher who receives personal health information about an individual from a health information custodian under subsection (1) shall, (e) not make contact or attempt to make contact with the individual, directly or indirectly, unless the custodian first obtains the individual's consent to being contacted, <u>except where the researcher receives personal health information from a custodian that is a prescribed entity mentioned in subsection 45(1) of the Act</u>; We assume that subsection 44 (6)(e) is intended to achieve an ethical aim: to protect individuals from being contacted by an unknown researcher "out of the blue," unless the HIC (e.g. physician, clinic or hospital) with whom the individual has an existing patient-provider relationship first asks the individual's permission to being contacted. Unlike with physicians, clinics or hospitals that deliver care and have established relationships with individuals, ICES and other PEs have no existing provider

	relationship with Ontarians, especially one rooted in trust. To be contacted directly by ICES is, in a sense, to be contacted by a stranger. ICES is not advocating for researchers to be able to use PHI to contact individuals directly out of the blue. We are in favor of relying on REBs to determine an ethically acceptable approach for contact and recruitment. Based on our experience, REBs generally advise that researchers rely on a member of the individual's "circle of care" to recruit for research. Only infrequently and in research that poses minimal risk to individuals do REBs permit researchers to carry out recruitment themselves. Regardless, we believe the method of contact and recruitment is an ethical matter best suited for REBs to consider and advise what is appropriate given the nature of the research.
Use Cases	**Improving Kidney Care for At-Risk Patients: A Patient Contact Pilot Study** There is data available at ICES that can be used to identify patients who are sick and who may not be receiving the best care. ICES can also identify patients who are receiving care that may be harmful to them. There are well-known, validated algorithms that can accurately predict an individual's risk of reaching kidney failure in the next two to five years. These algorithms use results from common laboratory tests for older adults, including estimated glomerular filtration rate (measured from serum creatinine) and urine albumin-to-creatinine ratio. Using administrative data, we can see patients who are at high risk for kidney failure. These patients with compromised kidney function are also at high risk of drug toxicity, and we often see prescribing errors in the datasets. Therefore, we know that these patients are declining but the medical community cannot intervene because it is challenging in the current model to re-identify patients and contact them or their providers directly and provide the necessary health information. For more efficient delivery of care, it would be highly valuable to develop a mechanism through which we can notify physicians (or directly notify patients) when we identify high-risk patients, especially those with medication errors. The ability to prevent patients from reaching kidney failure and developing serious adverse drug reactions can lead to significant savings for the Ontario health care system by preventing unnecessary hospitalizations, crash dialysis starts (i.e. patients who start dialysis in the hospital rather than an outpatient setting), and prolonging the need for dialysis. This model would also save patient lives. PEs have broad authority to collect health data for the purposes outlined above. Once the data have been collected, however, restrictions on how that data can be disclosed restricts the ability of PEs to use that data to support patient clinical care. The provision in *PHIPA* that allows for patient contact for research purposes tends to not align particularly well with the PE model. Given that the purpose of subsection 44 (6)(e) in *PHIPA* is presumably to ensure initial contact with a prospective research participant by someone with whom the individual has a familiar, pre-existing relationship, the requirement for the disclosing HIC to first obtain the individual's consent to being contacted misses the objective of this provision when the PE is acting as the disclosing HIC. For this patient contact study specifically, the challenges with this provision has led to lengthy project delays of almost two years, and has simply resulted in the actual originating HIC acting as ICES' agent, thereby satisfying the requirement of subsection 44 (6)(e) while also satisfying somewhat the intention to act as the familiar point of first contact. In reality, these agent agreements have resulted in extremely complicated flows of PHI during which the same members of the team are, at different points throughout the project, acting as ICES Agents, HICs and researchers. These complications detract from the overall intention of subsection 44 (6)(e) and in no way afford any additional privacy protections to prospective research participants.

THEME	d) STRENGTHENING PAN-CANADIAN ANALYTICS BY LEVERAGING EXTRA-PROVINCIAL DATA FOR HEALTH CARE PLANNING
Health System Goal	A health system that utilizes analytics and learnings from other provinces to deliver the most effective care to Ontarians.
Data Goal to Support Health System Goal	Authority to collect data from other jurisdictions outside of Ontario for analytic purposes and not just research, as is presently permitted.
Current Legislative Barriers	PEs cannot easily collect and use PHI and/or PI from other jurisdictions for analytic purposes. This creates similar "research by default" issues as identified above, since a PE's use of PHI for analytics is authorized only when collected from HICs.[2] A related challenge with "research by default" is the ongoing use of PHI as a persistent data holding. PHI disclosed to a PE under the research provisions of *PHIPA* and other Acts requires REB approval, which typically involves a fixed end date for use of the data. Compliance with REB approvals, then, ultimately results in successive REB amendments by the disclosing party, which carries with it the requirement to be constantly in the know of any revisions to the REB approval relating to use of the data.
Proposed *PHIPA* Amendments to Realize Health System Goal	Expand permitted disclosures of PHI to PEs for analytic purposes to those authorized under another Act of Ontario or Canada to disclose for analytic purposes, which in turn would strengthen pan-Canadian analytics, such as the Health Data Research Network Canada ("**HDRN**"). **Specific legislative revisions**: Revise section 45 (Disclosure for planning and management of health system) to include organizations and persons outside of Ontario who can disclose PHI to a PE for analytic purposes about the health system or health care more generally in Canada.
Use Cases	**Canadian Longitudinal Study on Aging ("CLSA")** CLSA is a national, long-term study that collects individual-level information about the biological, medical, psychological, social, lifestyle and economic aspects of people's lives. CLSA data is available by request to organizations like ICES. The purpose to which ICES would put CLSA data more clearly aligns with analytics than research; however, since CLSA is not a HIC, the disclosure of CLSA data to ICES must be for a "research by default" purpose. Not only do research requirements often add one-time additional resources, such as those necessary to secure REB approvals, ICES' ongoing use of CLSA data as a persistent data holding is necessarily impacted by the requirement to constantly amend its ongoing REB approval, despite the purpose of ICES' use of the data and its standing as a trusted data steward remaining constant. Since the very

[2] This challenge is further complicated insofar as *PHIPA* provides a definition of research without corresponding definitions of analytics, analysis, evaluation, etc. This definition of research – "a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research" – includes several elements that a commonly understood definition of analytics or evaluation would also include. This further blurs the line between research and non-research activities, especially for those who lack familiarity with interpreting complex legislation like *PHIPA*.

	purpose of projects like CLSA is to measure long-term health factors (in this case, for at least 20 years), changes in research requirements or REB approvals over time that could impact the ongoing availability of the data is directly at odds with the purpose of such long-term studies, and negatively impacts ongoing opportunities for pan-Canadian analytics that could provide unique insights toward improving Ontario's health care system.

THEME	**e) ADOPTION OF NEW TECHNOLOGIES FOR A MORE EFFECTIVE LEARNING HEALTH SYSTEM**
Health System Goal	A learning health system that is innovative and uses the most data-protective practices available.
Data Goal to Support Health System Goal	Ensure optimal levels of data quality are available for analytics and research purposes, while using data innovatively for education and training purposes, such as for the creation of synthetic data and the interoperability of data.
Current Legislative Barriers	Under *PHIPA*, a PE's use of PHI is limited to analytics and research. Certain basic uses of PHI are afforded to HICs under section 37 of *PHIPA* that appear to have been overlooked for PEs and which are inherent to the optimal functioning of any organization that holds data. For example, PEs are currently not expressly permitted to use PHI for data quality or data improvement activities, for education and training of its agents, or to modify the data so as to conceal the identity of the individual, e.g., the creation of synthetic data or modern advanced analytics, including artificial intelligence and machine learning ("**AI/ML**"). Creating synthetic data first requires real data from which the synthetic data can be derived.
***PHIPA* Amendments to Realize Health System Goal**	Some analytic and research projects could be facilitated without the use of PHI, relying instead on privacy-protected data such as synthetic data to develop and test new algorithms and models. **Specific legislative revisions**: Amend section 37 to allow a PE to use PHI for the following purposes: • 37 (1)(d): for the purpose of risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the custodian; • 37 (1)(e) for educating agents to provide health care or for analytics or research; • 37 (1)(f) in a manner consistent with Part II, for the purpose of disposing of the information or modifying the information in order to conceal the identity of the individual; Amendments to *PHIPA* that could facilitate data linkage include: • Incorporating provisions that encourage collection of PHI in such a way as to increase interoperability of data; and • Incorporating provisions that encourage all entities governed by *PHIPA* to develop a strategy for governance of their data that aligns with a vision of the health sector as a data-driven health sector.

Use Cases	Synthetic data has an expanding potential utility as this area further develops. With proper statutory authorization, PEs are well positioned to support these innovations and also maximize these benefits for Ontario's health system.[3] Such areas of use include: • **Advanced Analytics:** AI/ML techniques generally require large amounts of data, including full population data, quasi-identifiers, and full health histories, which poses challenges for data minimization. Synthetic data has the potential to reduce privacy risks associated with advanced analytics. • **Education/Training:** Synthetic data can be useful in developing data science and analytic skills among students, trainees, and even external researchers. This training could include courses, workshops, or other training activities that are separate from specific research and analytic projects. • **Machine Learning Model Development and Testing:** Machine learning models may retain the data used to train them after they are removed from secure analytic environments to be validated on other datasets. Use of synthetic data for these purposes can reduce data security risks. • **Project and Analytic Model Development:** Some projects can benefit from being developed and/or piloted using synthetic data prior to obtaining approval to access PHI. • **Data Engineering and Software Testing:** Synthetic data can provide a realistic but privacy-preserving option for developing and testing new systems and software, including scenarios where third-party service providers are engaged to perform work on these systems. Use of synthetic data would also increase capacity for ICES resources and create efficiencies since privacy assessments and data sharing agreements required for accessing PHI would not be applicable. While recognizing the promising opportunities for use of synthetic data, there remains key benefits for use of PHI by ICES in supporting the learning health system and improving data quality. Training analytic staff in data management and statistical techniques is critical to the quality of analytics and research projects undertaken by ICES. In addition, using PHI to validate and improve the PHI itself ensures improved data quality, leading to more accurate insights from analytics and research and then better-informed decision-making in the health system.

In turn, to modernize the issue of compliance requirements, we now set out ICES' high-level commentary on how the IPC Manual can be augmented to support the evolving technology and cybersecurity landscape, as well as with compliance requirements that, in our view, do not impact the privacy or security rights of individuals.

[3] As noted above, making synthetic data widely accessible to a PEs staff, students and external researchers would facilitate training and application and computer code development, and would avoid the unnecessary burden of project-level requests for data access. Such datasets are widely available for these purposes in other jurisdictions, e.g., https://www.cms.gov/Research-Statistics-Data-and-Systems/Downloadable-Public-Use-Files/SynPUFs.

4. IPC Manual and Compliance Requirements

There is an unlevel playing field in Ontario today in the rules and regulations governing analytics and research. Compared with HICs, PEs are under stricter compliance regimes, have fewer authorities to collect, use and disclose PHI, and are subject to greater external oversight. At the same time, some HICs are collecting PHI from multiple other HICs to create data repositories for quality improvement, analytics and research purposes rather than for direct patient care. In our view, PEs should have the same authorities and not be subject to substantially stricter regimes than HICs that are able to carry out the same activities.

Similarly, the optimization of a PE's compliance and security regimes requires recognition of a constantly evolving threat landscape and equally responsive security technologies. There is an opportunity to inject greater flexibility into the IPC Manual to ensure that a PE's compliance and security obligations are aligned with internationally recognized standards. This will ensure that a PE's available security measures can be persistently updated to ensure optimal responses to the needs of Ontario's health system.

The following sections provide high-level overviews of opportunities to modernize compliance and security requirements, particularly with respect to cybersecurity mandates.

Overall, opportunities to modernize compliance and security requirements include the following:

i. Embracing simplicity for data sharing;
ii. Allowing for cutting-edge cybersecurity practices;
iii. Embracing simplicity for privacy breaches;
iv. Better facilitating multiple designations through consistency of terminology; and
v. Simplifying indicators reporting in the IPC triennial review process.

Below is each key theme further assessed and explored.

THEME	a) EMBRACING SIMPLICITY FOR DATA SHARING
Health System Goal	Better use of resources to allow for more time spent on complex health privacy matters rather than routine transactional work.
PE Goal	Simplify the time and effort required to collect, use and disclose data between parties by adopting digital and umbrella Data Sharing Agreements ("**DSAs**") where possible, particularly where DSAs are with individual health care providers such as physicians, and a large number of DSAs are required to ensure data are representative of the broader population.

IPC Manual Section	**16 – Policy and Procedures for the Execution of Data Sharing Agreements** **Note:** there is nothing we would revise for this section; rather, we are advocating for the government to support a wider initiative, working in collaboration with the IPC and other stakeholders, to leverage technology to simplify these types of transactions.
Use Cases	Collecting primary care electronic medical record ("**EMR")** data for population-level analytics often requires collection of PHI from all primary care physician HICs across the province. Due to the high volume of transactional work required to support such an endeavour, it is not feasible to execute and/or update one-off DSAs with every participating HIC. It would be ideal if the MOH supports (e.g., hosts or funds) digital infrastructure that can be leveraged to build DSAs with standards terms and conditions for individual physician HICs. This is similar to "shrink-wrap" contracts, which are boilerplate contracts packaged with tech products, and use of the product is deemed to be acceptance of the contract's terms and conditions. There would be an opportunity for the physician HIC to read, review, accept, and "e-submit" the DSA back to the PE. The same approach could be undertaken with respect to pharmacists and other types of regulated health professionals who meet the *PHIPA* definition of a HIC. In the future, a digital DSA infrastructure also could exist for all HIC-related agreements. Of course, legal review still would be needed before negotiating terms and conditions and signing, where applicable. But in situations where there is little negotiation needed or where an umbrella agreement already has been negotiated by the parties, additional data schedules could be easily added within the digital infrastructure system.

THEME	**b) CUTTING-EDGE CYBERSECURITY PRACTICES**
Health System Goal	Enable a cybersecurity program that is agile and responsible to global threats to avoid strains on the health care system.
PE Goal	Facilitate timely updates to policies and procedures in response to ongoing cybersecurity threats by adopting international standards and frameworks, such as the National Institute of Standards and Technology ("**NIST**") cybersecurity framework, rather than prescriptive security requirements in an IPC Manual that is not updated on a regular basis to be current with a constantly evolving threat landscape.
IPC Manual Section	**Part 2 – Security Documentation**
Use Cases	Continued compliance with the IPC Manual's cybersecurity obligations poses several unique challenges rooted in its application to PEs only, and the fact that it exists as a largely unknown standard in the wider information security industry. Due to the relatively niche scope of the IPC Manual, a significant amount of time is allocated to training information security personnel and consultants, many of whom may have extensive experience in the Ontario health care landscape. Additionally, when communicating with potential data partners and stakeholders, compliance with internationally recognized standards is often a desirable state, as such compliance measures the breadth of an organization's information security program. The limited scope of application of the IPC Manual only results in uncertainty and confusion. While PEs are considered part of the Ontario health care system, even HICs are frequently unfamiliar with the IPC Manual and its requirements.

	Adoption of an internationally recognized standard such NIST or the International Organization for Standardization ("**ISO**") would provide PEs with the following benefits: • **Trust:** A PE's compliance with an internationally recognized standard would demonstrate its ongoing commitment to information security and the critical role it plays in securing the data entrusted to it when communicating with industry stakeholders. This demonstrates to stakeholders that the PE satisfies a defined set of standards and requirements that are known and understood internationally across the industry, and that the PE's policies and practices are routinely evaluated against current threat landscapes. • **Agility:** As information security and threat landscapes evolve, industry standards are frequently updated to reflect these evolutions, avoiding the need to maintain policies and technologies that are outdated and ineffective. Further, the adoption of an internationally recognized standard would allow PEs to focus more on achieving its objectives, rather than simply demonstrating how those objectives are achieved. • **Consistency:** A key benefit of leveraging established standards published by internationally recognized bodies is that the language and controls included in these standards are understood consistently across the industry. The broad support and recognition of these standards by technology vendors and service providers results in improved adoption due to the resources available. Given the current resource constraints ICES faces, and considering that compliance with any standard, including the IPC Manual, is a resource-intensive endeavor, focusing cybersecurity compliance instead on an internationally recognized standard would yield a greater return on its investment while improving the quality of cybersecurity it can provide.

THEME	**c) EMBRACING SIMPLICITY FOR PRIVACY BREACHES**
Health System Goal	Better use of resources to allow for more time spent on complex health privacy matters instead of routine compliance work.
PE Goal	Inject flexibility into compliance requirements by narrowing the definition of privacy breach to incidents only where an individual's privacy is impacted or at risk, rather than other types of non-compliance matters that may arise from contractual, policy or procedures breaches.
IPC Manual Section	**29 – Policy and Procedures for Privacy Breach Management**
Use Case	The IPC Manual requires a PE to define a privacy breach as a contravention of privacy policies, procedures or practices, as well as contravention of agreements that relate to the collection, use and/or disclosure of PHI. This overly broad definition can result in circumstances in which a contravening incident meets the definition of a privacy breach while having no impact on an individual's privacy. For example, many of ICES' DSAs include a requirement to acknowledge the data provider in any journal articles based on ICES studies. If ICES overlooked inclusion of such an acknowledgement, this would qualify as a privacy breach despite having no impact whatsoever on privacy or ICES' information handling practices.

	When incidents like this must be handled as privacy breaches, ICES must then follow comprehensive requirements dictated by the IPC Manual, as well as its privacy breach policy and procedures. This requires investigation, containment, notification, remediation, etc. To be sure, such requirements are appropriate for actual privacy breaches in which individual privacy and confidentiality of PHI are impacted. But similar requirements for compliance incidents that do not impact PHI results in a suboptimal use of ICES' resources (e.g., its time and expertise) that otherwise would be focused on actual privacy-related matters. Incidents unrelated to privacy should be treated as breaches of policy or contract. They should not be understood as privacy breaches.

THEME	**d) FACILITATING MULTIPLE DESIGNATIONS THROUGH CONSISTENCY OF TERMINOLOGY**
Health System Goal	Broader understanding of the health system through PE and EMDIU designations
PE Goal	Align definitions in the IPC Manual, Addenda, and the Ontario Public Service Data Integration Data Standards (the "**Data Standards**") to allow for consistency across policies, procedures and practices.
IPC Manual Section	**24 – Policy and Procedures with Respect to De-Identification and Aggregation**
Use Case	Although defined consistently in *PHIPA* and *FIPPA*, the term "de-identified" appears to be treated differently in the PE Manual and the Data Standards. The PE model adheres to the legislative definition, whereas the Data Standards appear to treat de-identification as existing somewhere along a spectrum. This inconsistency makes data sharing between an organization's PE and EMDIU "zones" conceptually difficult, as the same data may be seen as simultaneously identifiable and de-identified. If it is the intention for EMDIUs that are also PEs to treat de-identification as somewhat subjective, it should be understood consistently across its manuals.

THEME	**e) SIMPLIFYING INDICATORS REPORTING IN THE IPC TRIENNIAL REVIEW PROCESS**
Health System Goal	Better use of resources to allow for more time spent on complex health privacy matters instead of routine compliance work
PE Goal	The IPC Manual outlines over 50 indicators that a PE must report as part of the Triennial Review process. Many of these indicators are associated with a PE's higher-risk activities with regard to collection, use, disclosure, and security of PHI. There are opportunities, however, to streamline these indicators to focus on higher-risk areas while eliminating reporting of lower-risk matters, thereby freeing up resources currently required for the ongoing tracking and preparation of lower-risk indicators.
IPC Manual Section	**Appendix "C" – Privacy, Security and Other Indicators**
Use Case	For examples of lower-risk indicators, the IPC Manual currently requires: a) For all privacy policies and procedures, • The dates they were reviewed since the last Triennial Review process;

	• A description of any amendments made to the policies and procedures; • A description of any new policies and procedures implemented; • The dates that new and amended policies and procedures were communicated to agents of the PE, and the nature of the communication; and • A description of any amendments made to communication materials available to the public and other stakeholders. b) For all security policies and procedures, • The dates they were reviewed since the last Triennial Review process; • A description of any amendments made to the policies and procedures; • A description of any new policies and procedures implemented; • The dates that new and amended policies and procedures were communicated to agents of the PE, and the nature of the communication; and • A description of any amendments made to communication materials available to the public and other stakeholders. c) Other low-risk indicators: • The dates and a description of communications to agents in relation to privacy; • The dates and a description of communications to agents in relation to information security; and • A description of amendments made to Statements of Purpose. These indicators are not information that PEs currently need to log for compliance with other sections of the IPC Manual. They require additional resources and effort exclusively for compliance reporting. PEs are encouraged to entrench privacy and security matters into their operational culture through activities like regular and ongoing communications with agents and through regular reviews of policies and procedures. But requiring separate indicators to track each instance of these activities and their description makes it more challenging and time consuming, which can have a chilling effect on the actual work itself of the PE. In many instances, ICES has the information in our systems that is required for indicators reporting, but often the information needs to be aggregated in a suitable format to specifically respond to an indicator's specification. Once again, it is a resource-intensive process that takes away time and expertise from higher-risk matters.

Over the course of 2022, ICES worked with other PEs and Prescribed Persons ("**PPs**") to provide consolidated feedback to the IPC regarding their proposed revisions to the IPC Manual. This feedback to the IPC was provided in two joint submissions prepared over a months-long period of careful review of the proposed revisions to the IPC Manual, and involved ongoing discussions amongst the PEs/PPs. Providing consolidated feedback to the IPC demonstrated that the IPC Manual is foundational to the privacy and security programs of all PEs/PPs, and it impacts business operations and the ability to deliver on mandates and existing commitments. As such,

the PEs/PPs recognize the importance of providing meaningful and coordinated input for these and future changes to the IPC Manual.

For a copy of the consolidated feedback to the revised IPC Manual submitted by PEs/PPs on June 15, 2022, and our additional feedback submitted on October 28, 2022, please contact us. If the MOH wishes to discuss this feedback in more detail, ICES is happy to participate in these conversations.

CONCLUSION

If the health care data necessary to support health system evaluation, planning and monitoring continues to exist in its current siloed form, Ontario will continue to have a fragmented health system that is unable to appropriately respond to the needs of Ontarians. The MOH, in alignment with the IPC, should consider broader legislative authorities for statutory entities that have existed since at least the inception of *PHIPA*. These entities have earned the trust of health system stakeholders, scientists, community-based organizations and the wider public. They have also made great strides in safeguarding PHI and PI by embedding privacy and security practices in their day-to-day operations. Through the oversight of the IPC, PEs have obtained approval of their policies, procedures and practices every three years, fully meeting and demonstrating their accountability and trustworthiness to Ontarians. By operating as a trustworthy data steward, ICES and other PEs are well-suited to continue to be key allies in government's mandate to improve the health system.

CONTACT US

Privacy & Legal Office (PLO) @ ICES

Chief Privacy and Legal Officer
Rosario Cartagena
Rosario.Cartagena@ices.on.ca

Director, PLO
Michael Smith
Michael.Smith@ices.on.ca

General Inquiries: privacy@ices.on.ca

APPENDIX "A"

ICES is among the lowest cost centres in Canada in routinely providing secure access to population-level health data, and is one of the most comprehensive health data repositories available globally.

We have 110 data holdings and collect dozens of datasets annually for project-specific purposes.

Our data holdings include data related to health services; health care providers; population and demographics; health surveys; clinical trials; environment; immigration, refugees, and newcomers; primary care and specialist electronic medical records; genomics; and medical imaging, among others.

In the 2021/22 fiscal year, we had 365 new and 1,183 ongoing ICES projects. We also had 117 requests to disclose to third-party researchers.

Before any single project can begin, a privacy impact assessment ("**PIA**") must be conducted to ascertain whether ICES can legally collect, use or disclose the PHI being requested. As a result of the high-volume of services requested and the diversity of available data, there is a high demand on privacy services requested.

In respect of the day-to-day operational work supported by Privacy Services in the Privacy & Legal Office, we have:

- 1 Privacy Manager;
- 1 Sr. Privacy Analyst; and
- 1 Privacy Analyst (a role created during the COVID-19 pandemic)

The work of the Privacy Services team includes the following:

- **ICES Data Holding PIAs** – involves conducting analyses to confirm whether ICES has lawful authority to collect and use PHI that can be retained by ICES as an ICES Data Holding for use by other ICES Agents.
- **ICES Projects by ICES Scientists or ICES Agents** – involves reviewing several documents and conducting often complex analyses to confirm whether ICES has lawful authority to collect and use PHI for a specific project.
- **Disclosure of PHI to Third-Party Researchers** – involves conducting analyses to confirm whether ICES has lawful authority to disclose PHI to Third-Party Researchers for research purposes.
- **Suspected and actual privacy breach investigations** – involves investigation, containment, notification and remediation across departments and the wider ICES Network.

- **Privacy Consultations** – involves responding to questions and inquiries from agents across departments and the ICES Network, e.g., questions about business project development, process improvements, attending meetings with data providers, scientists and other key stakeholders, as well as conducting research to answer questions.

In ICES' Research & Analysis department, we also have four Research Program and Project PIA Coordinators. We also have four Privacy, Risk and Compliance Analysts who support the ICES Sites across Ontario. Their privacy work involves reviewing access requests to confirm whether ICES has lawful authority to use PHI that ICES already has as a Data Holding for a specific project.