ITAC Health
PHIPA Modernization Feedback

TO ONTARIO MOHLTC

FEBRUARY 21, 2020

Summary

At the conclusion of November 20, 2019 meeting hosted by the MOHLTC privacy policy team that included representatives from ITAC Health Board and members, an action opportunity was requested and permission received to share the Ministry's PHIPA Modernization document with select privacy subject matter experts within the ITAC Health membership. ITAC Health members, including SME members, have provided input that has been collected and summarized in this document. Our goal is to provide timely and in-depth feedback beyond the November meeting's initial reflections on the PHIPA Modernization policies. We appreciate the opportunity to contribute to the Ministry our summary that includes five sections in companion to this executive summary:

- thematic topics related to PHIPA Modernization;
- beyond PHIPA, privacy (and security) contextual discussion; and
- general comments, recommendations and questions on PHIPA Modernization;
- direct references to slide content in Ministry's PHIPHA Modernization deck;
- bibliography of external documents relevant to PHIPA Modernization effort

1. PHIPA Privacy Themes

- Roles and responsibilities under the new PHIPA
- Penalties Under the New PHIPA
- Consent – aligned with GDPR
- Patient access to information
- De-identification and secondary use
- Right to portability
- Right to be forgotten
- Breach notification
- Research Ethic Boards harmonization
- Governance operating model
- Levers for change to enable data sharing

Roles and responsibilities under the new PHIPA

- **Patient** - a natural person whose personal data is processed by a controller or processor
- **Health information custodian (HIC)** - a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed.
- Note: The term "custody and control" needs to be clear and specific in between HICs, vendors and patients.
- **Data Processor** - any person (other than an employee/agent of the a HIC) who processes the data on behalf of the HIC.

Penalties Under the New PHIPA

- financial penalties identified under the current PHIPA regulation:
  - 73(2) A person who is guilty of an offense under subsection (1) is liable, on conviction.
  - If the person is a natural person, fine of no more than $100,000.
  - If the person is not a natural person, fine of no more than $500,000.
- Make sure there are "teeth" to ensure compliance with PHIPA.

Consent – aligned with GDPR

- Consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes.
- It also requires individual ('granular') consent options for distinct processing operations.
- Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.
- Name any third party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.

Note: The current consent framework (4 levels) could be a barrier or challenge for vendors to implement and manage.

Patient Access to Information

Note: Consider establish requirements to be apply consistently for a third party to access information on behalf of a patient. The third party could be a vendor (e.g. Personal Health Record).

- Individuals will have the right to obtain:
  - confirmation that their data is being processed; and
  - access to their personal data
- Information must be provided without delay and at the latest within one month of receipt.
- **How to verify the identity** of the person making the request – some guidelines will be helpful
- If the request is made electronically, provide the information in a commonly used electronic format **(not just a PDF**).

De-identification and Secondary Use SA8

- Who can de-identify PHI?
- What are the requirements
- Should patients be informed?
- Enterprise de-identification tools, with ability to quantify risk for target audience, standardized creation of data sharing agreements
- To whom (vendors, researches, clinicians, policy developers, public, etc.) the de-identify PHI can be disclosed to? Reference CIHI's Health System Use Vision report of 2013.
- What's constitute secondary use? (refers to the comments of the IPC Ontario on Bill 128)
- ITAC Health letter to the editor of Globe and Mail, November 2019

Slide 8

SA8 De-Identification (Slide 9)
De-identification is a complex topic. Studies have shown that you can identify the person associated with anonymized data with simply gender, zip code, and age. However, when you consider some of the healthcare use cases — trying to understand public health issues, trying to pin down trends — these are data elements that are extremely important! If you were to remove zip code or neighborhood, for example, you might never arrive at the conclusion that there is a regionalized hazard which is causing diseases (such as proximity to a certain chemical plant or business).

For these reasons, many organizations implement a risk based approach. It's not possible to anonymize or de-identify the data perfectly, but it is possible to reduce the risk of exposure of personal information while still achieving the goals of the database project.

There are experts who can manage these risks and help organizations achieve their goals, but the question does arise, once again — who decides which approaches are acceptable? Who determines that one person is an expert and that their approach is valid?
Susan Anderson, 2020-02-06

Right to Portability (tie to access to information)

- The right to data portability allows individuals to obtain and reuse their personal health data for their own purposes across different services.
- It allows them to move, copy or transfer personal health data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- Must provide the personal health data in a structured, commonly used and machine readable form (**not just PDF**).
- May be required to transmit the data directly to another organisation if this is technically feasible (**interoperate standards must be considered for data sharing**)

SA9

Right to be forgotten (this could be a tough one for health care information as some information will need to be kept for a period of time).

- To enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. For example:
  - where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
  - when the individual withdraws consent.
  - when the individual objects to the processing
- There are some specific circumstances where the right to erasure does not apply and the controller can refuse to deal with a request. For example:
  - to exercise the right of freedom of expression and information.
  - to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
  - for public health purposes in the public interest.
- If an organization has disclosed the personal data in question to third parties, the organization must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

SA9 Right to be Forgotten (Slide 11)

In healthcare there are public health concerns, so typically information about a patient cannot be forgotten. Because healthcare has historically retained records for the long term, most electronic health record systems are not designed to facilitate the removal of all record of someone.

Within the health record system are structured data (fields such as name, DOB, address) and unstructured data (reports, scans of documents, and so forth) and this data is archived and removed from the live system. In the past, archiving might mean optical disk archives of the data. Today it is more likely to be cloud storage or removable disks. In order to remove someone from archived data would require someone tracking down all of the storage locations, retrieving them, and then removing that data. Typically such long term archival solutions are designed to prevent any alteration since they represent a legal record.

There are also extensive audit trails within the system — as required by law — showing activities performed on each patient's data (viewed, printed, edited, etc.) and by whom. To remove all trace of a particular person from the system would require going through those audit logs and removing all reference to them.

Susan Anderson, 2020-02-06

Breach Notification

- Keep the most recent updated PHIPA requirement on Mandatory Reporting.

Privacy Impact Assessment

- Conducting a PIA must be mandatory under specific circumstances. Example of Alberta's Health Information Act (HIA) legislation and PIA requirements.

Data Protection by Design

SA12

The new PHIPA must embrace the Privacy by Design (PbD) principles as PbD can be applied to technology, business practices and physical design.

7 foundational principles

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into design
4. Full Functionality – Positive-Sum, to Zero-Sum
5. End-to-end Security – Full Lifecycle Protection
6. Visibility and Transparency- Keep it Open
7. Respect for User Privacy – Keep it User-Centric

Slide 13

SA12 Data Protection by Design (Slide 14)

These are all great principles, but our concern is that organizations will vary widely. Some will think they are doing their due diligence and yet their solution may be inadequate. Others will take this very seriously and institute a great program.

- How do we make sure that there is a minimum bar that all must meet?
- How can the approach and the product both be validated?
- Who can be certified to make such judgements?

Software is notorious for the lack of standards as to how things should be done. There is no legal "license to code".

Susan Anderson, 2020-02-06

Governance for PHIPA SA2

- Exercise trust across jurisdiction through engagement in governance
- Data Stewardship Committee for oversight of PHIPA data sharing
- Dispute Resolution with accountability ultimately to Minister of Health
- Provincial Governance Secretariat and sustained funding

Slide 14

SA2 Governance for PHIPA- we recommend to use it for the entire healthcare value-chain

Susan Anderson, 2020-01-29

PHIPA Data Sharing – Levers for Change

- Step One: demonstrate capability of standards and technology to enable robust interoperability for custodial data transfers

- Step Two: Minister to mandate for creation of plans to expand data sharing according to well defined timeframe(s) by the Ontario Professional Colleges for the custodians of patient's health data

Research Ethic Boards Harmonization &Reciprocity within Ontario and Beyond

- **Research ethics: are we minimizing harm or maximizing bureaucracy?** A phenomenon called "ethics creep" is discouraging researchers rather than protecting study participants (ref: bibliography)
- Example of Alberta REB for health designation by Minister to harmonize Health research ethics boards and encourage reciprocity across these REBS to expand research capacity.

Supplemental Feedback

PHIPA Should align with General Data Protection Regulation (GDPR)

- The GDPR represents the latest iteration of privacy law in the new world of the Internet, mobile, cloud, machine learning, artificial intelligence, IoT and other advancements in technology and data science.

- This will help vendors to build privacy and security controls into their products/solutions not only for the Ontario Market but international market.

Data Security

- Required to "implement appropriate technical and organizational measures"
- Must be prescriptive. For example, HIPAA security rules provide a clear guidance for cover entities to comply with HIPAA.
- Should consider using an international security standard framework such as ISO

ISO Standards

- ISO – 27001/2 (Code of Practice for Information Security Controls)
- ISO – 29151 (Code of Practice for personally identifiable information protection)

ISO

Ontario Privacy Legislation & Open Data

- Personal Health Information Privacy Act (PHIPA) – expand appropriate access to custodian held data for health system use
- Personal Information Protection and Electronic Document Act (PIPEDA) – opportunity for harmonization between federal and jurisdictional privacy legislation.
- Freedom of Information and Protection of Privacy Act (FIPPA) – ensure harmony with PHIPA
- Open Data First – assumption that new data sets are to be open, and only closed with sufficient argument to withhold for privacy protection.

Cloud First Strategy, Recommendations

- The pattern of Privacy hindering Access and Innovation, and, as a result, the ability to deliver better care faster, has been consistent throughout our interactions with the healthcare sector, and the government of Ontario in the past four years. The concern with cloud security has been especially prominent as a reason for hesitation to embrace the cloud.
- In reality, major cloud providers can guarantee higher levels of security and protection from cyberattacks than any health organization can afford individually. They hold industry security and privacy certifications, and operate data centers with protected B status.
- Cloud is the greatest technological enabler of innovation, faster digital transformation, and integrated health care, at a lower cost and with greater security. Cloud is mature; it enables highly performant de-identification of personal data, data integration, and machine learning to be used for enabling integrated care through data exchange and research purposes while providing data governance, and identity and access management.
- Overcoming hesitancy to adopt the cloud by providing cloud framework and path for digital transformation can be seen one of the most effective steps towards faster adoption of integrated health care.
- We encourage such recommendation for developing and mandating cloud-first framework for supporting digital innovation in Ontario's healthcare:
  - for individuals to view and share their Personal Health Information from custodians directly through consumer electronic service providers
  - when establishing a review capability regarding the use of Personal Health Information or de-identified information for research / innovation purposes that benefit the public

Patient Charter of Rights

- Explicitly identify rights and remedies possible by patients when their privacy of personal health data has been misused under control of Ontario custodian.
- Clarity on public patient's ability to capture, collect, use and disclose their own health data without constraint by government privacy legislation or interpretation by custodian.
- Example by Alberta to create new Alberta Health Act (addressing gaps in Canada Health Act) and companion Patient Charter of Rights

3. General Comments, Recommendations on PHIPA

- Our current understanding around interoperability frameworks are that many healthcare applications and physician EMR's are not based on an open API framework, thus making it difficult for data to flow across organizations. The ministry may want to consider legislating a requirement for healthcare applications to be based on open APIs.
- Further to this, the creation of a centralized and integrated healthcare portal may help in making data accessible and available from anywhere. Patients and families should not be required to log into provider specific portals to access different portions of their health records. There should be one comprehensive unified EMR that patients and caregivers can access to obtain a integrated view of their health record. SA3
- Another piece of consideration is in the area of patient access to data. We believe that from the patient side, access should be seamless to one's own health data. Of course privacy concerns may arise in this area, and as such enablers such as two factor authentication can be used to ensure proper protection is in place. With regards to formal patient data requests, this feels like an area that could benefit from increased automation to improve response times. SA4
- Provide clarity on whether the recommendations all relate to a proposed legislative change, or could mean a policy change or voluntary guidance document released by the Ministry.
- Specify the purposes, and types of organizations, related to the new data sharing recommendations (where not already specified).
- Where recommendations indicate new data sharing opportunities, provide a corresponding recommendation for transparency and safeguards.
- Consider a recommendation for time-limited data sharing across organizations for approved health data integration purposes (e.g., establishment of shared health information systems, OHT planning, agency consolidation), which would expire once the integration project is completed.

Slide 23

SA3 Slide #18- 2nd Bullet-A central Portal can be easily breached via rainbow table attack. Suggest perhaps accessing encrypted material and ensuring the communications tools is encrypted at both at rest and transit and that the keys for the encrypted tools are not stored on the server. Because most email wrappers have this flaw- if the server is breached, it is easy to access the entire server by utilizing the keys that are centrally stored.
Susan Anderson, 2020-01-29

SA4 Slide#18-3rd Bullet-Multifactor authentication should be employed while utilizing a tool that is not only encrypted at rest but also in transit to ensure security!!!
Susan Anderson, 2020-01-29

General Comments, Recommendations on PHIPA (con't)

- Provide a more detailed recommendation on the role of the Patient Ombudsman for complaints or decision-making with respect to public interest use of data.
- Provide a recommendation to develop a senior health data governance role and committee.
- Provide recommendations that enable patient choice (e.g., an opt-out mechanism for the secondary uses described in the recommendations).
- Provide more details on the recommended role of the "integration unit" and the contents and form of "integrated data". For example, should the "integration unit" lie within the Ministry of Health, within the OPS or BPS, or be hosted by one or several HICs (and/or their service providers)? Would integrated data be used only in a de-identified form?
- Provide a recommendation to develop a standard or guidance document on health information de-identification and anonymization.
- Provide details on the IPC's review capabilities under these new recommendations, including any expected role in the review of use of de-identified or anonymized information, and possible streamlined, risk-based reporting tied to new data sharing or data integration initiatives.

General Comments, Recommendations on PHIPA (con't)

- Privacy requirements must be clearly defined. Otherwise, these will be subjected to different interpretations and make it very difficult for data sharing , enable innovation and respect patient's privacy rights.
- Out of country cloud computing/hosting provider. Provide clear requirements to enable this kind of services.
- Should consider creating a "Governance Body" for dispute resolution for any issues pertaining to the implementation or interpretation of PHIPA requirements.
- Was also interested in the "willful deidentification" penalty. In my research, I know nationally we do not have any standards on how data should be deidentified. So although I agree it should be discouraged, we would need a standard by which data is considered deidentified. This also touches on the topic of destruction of data as well with practices such as crypto shredding.
- Also, there is no specific mention of public cloud use guidelines. That will be SA13 a key component to how technology partners engage with the OHT's as well as the OHT's develop digital strategies. What we don't want is a lowest common denominator framework that does not encourage innovation or adoption of current computing deployment strategies. There is a real danger of stepping backwards

Slide 25

SA13 Public Cloud (Slide 20)

Moving to the cloud has security and privacy benefits, but it certainly makes sense to keep the data “in country”. There are many legal and political* reasons for this. This is well recognized by cloud providers, and leading cloud providers — such as google — make it easy for administrators to restrict data to specific regions and zones.

*Note: In addition to the many data breaches that were occuring, “surveillance capitalism”, and NSA spying were motivations behind introducing additional privacy laws.

We also agree with other stakeholder feedback that clear requirements for out of country cloud computing/hosting provider is needed, as well as well-defined public cloud use guidelines.

Susan Anderson, 2020-02-06

General Comments, Recommendations on PHIPA (con't)

- The one big topic that I do not see covered is "Circle of Care" and consent directives ... the reality of an aging population is creating more volume and driving cost up... the goal is to keep people out of hospitals and to do that the system overall must depend more on the generosity of friends and loved ones... I'm sure we have all played a Caregiver role to our loved ones within our day to day lives... and I think the legislation needs to give more guidance on this point... should define the term and how it would work, no different than it defines research and secondary use...
- Modern legislation must empower Patients to be able to give strong consent directives to enable their circle of care to support them without getting a lawyer involved... and more importantly, the providers within the system must be given these directives as the frontline team is trained not to share with anyone other than the patient... and therefore if this needed change was better adopted the frontline teams would need clear support from the legislation to support their actions...
- While all parties support the concept of increasing patient and HCP access to health data for better health outcomes, this must be balanced with the concept of informed and meaningful consent. More specifically:
- There is a need for patient opt-out mechanism to respect individual choices. Similarly, consent should not be "all or nothing"; the individual should be able to consent to some aspects of sharing, but refuse others (for example only, to agree to share PHI to all HCPs within their circle of care, but refuse consent to have their data, even if de-identified, share with Ontario Health for research or planning purposes).
- The provision of care should not depend on whether the patient has provided consent for sharing of their information.
- Where consent is obtained, there is a need for the ability of custodians to easily demonstrate to third parties, such as insurers or claims processors, that individual has provided it (and that the consent covers the information that may be requested by such third parties)
- This document seems to be very high level and aspirational at the moment. It hard to comment on from an IT service provider perspective. However, the feedback/questions I've received from my team is whether the Province intends to consolidate integration of the service provider and IT/technical standards? In this vein, it would be extremely beneficial for ITAC to be able to participate in development of IT/technical standards associated with a shared HI system. The status quo seems to be seeing those for the first time in the course of RFPs which makes it challenging to retrofit COTS software and solutions.

General Comments, Recommendations on PHIPA (con't)

- Proposed amendments to enable providers to more easily share information with other providers to support individual patient care as well as public and population health. Authorize prescribed registries and entities to disclose Personal Health Information to Health Information Custodians for the purpose of quality of care improvement initiatives (e.g. sharing Personal Health Information on emergency room readmissions across custodians).

  Comment:

  - Ensure traceability of information disclosures within and across circles of care for
    - the improvement of care for the individual
  - vs
    - de-identified information for pathway lessons learned

  Distinguish between care initiatives and admin initiatives

- Proposed amendments to enable Government to make better decisions through data-driven insights.
- Authorize a unit of the Ministry of Health to collect, integrate and de-identify Personal Health Information from prescribed registries, prescribed entities and health information custodians purposes of planning, management, delivery or evaluation of health programs or services, and for research purposes.
- Create the ability for integrated data to be available to researchers for analysis to support management, planning, evaluation and monitoring of health services or other programs and services, and research purposes.

  Comment:

  - De-identifying data across sources to create a digital twin of a patient's care journey
  - would need strict rules/controls to restrict identification of the patient with an appropriate offence for doing so willfully

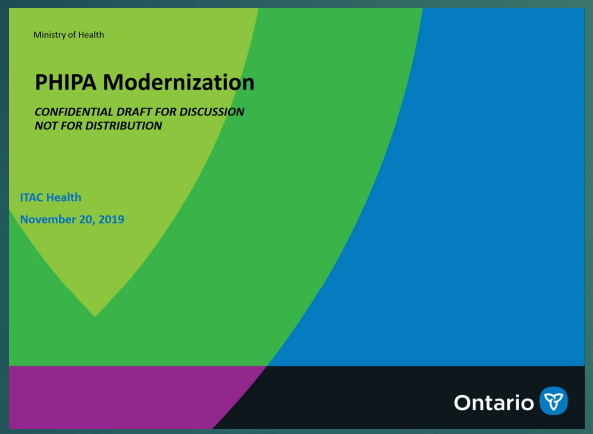
General Comments, Recommendations on PHIPA

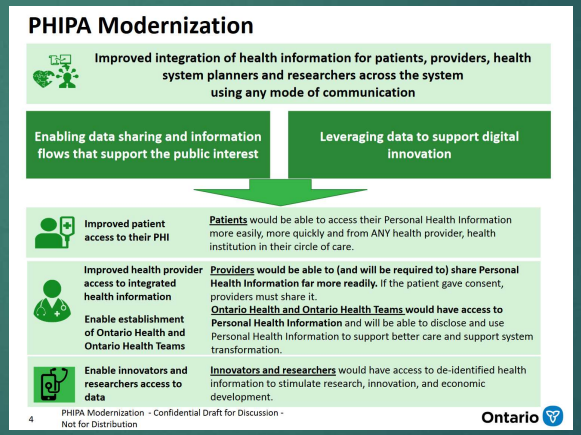
- There are no shortage of requirements and guidelines applicable to health care providers with respect to the appropriate use and safeguarding of personal health information. However, these obligations are sometimes overlapping and create confusion and challenging administrative burdens for provider practices and ultimately result in some degree of uncertainty for providers, patients, researchers and other stakeholders. PHIPA modernization presents an opportunity to clarify, simplify, and ease access to health information for care providers -whose access is the reason this information is collected in the first place. Attention must be given to potential intrusions into commercial intellectual property rights of a variety of stakeholders - and may disrupt the work of clinicians, research bodies, universities, vendors and other third parties
- Barriers to Patient Access. It is imperative that those legislating amendments to PHIPA align with other regulatory requirements that exist in the health care system and balance the practical realities that available technology offers and the cost and administrative burden changes may place on both patients and physicians. Many health care providers balance a multiplicity of technology systems and paper records and the policy environment must continue to address this fact. Further engagement with appropriate organizations (OMA, IPC, CPSO) to set policies with respect to fees and response time may assist with reducing the barriers identified by the Ministry. The government could consider funding incentives for organizations so that they may continue to develop products and work alongside Health Information Custodians (HICs)and researchers to identify how digital solutions can improve their practices and increase proficiencies within the industry. Vendors will be better able to address the concerns posed by the government as they have the ability to develop solutions to those problems.
- Patients are likely to be unaware that all their information is accessible by government regardless of masking –they are likely to assume that the masking at the provider level will be preserved. If patients find out that the government has access to all their personal health information regardless of masking, they might be likely to withhold disclosing PHI to their provider. If providers are not provided with sufficient information, patient care could be compromised. Public confidence and trust in the system could be compromised. De-identification should be carried out on an arms-length basis, outside of government itself, not by an agency of government.
- Except in limited appropriate circumstances there should be no overarching access right to PHI; there must be checks and balances in place to ensure that the government and government enabled establishments are not misusing information and that patients continue to have rights over their data. There must also be limitations on the ways in which this data is used in order to protect patients. For example, without proper security measures and legislative restrictions, entities such as insurance companies could use health data to discriminate against specific cohorts of the population.

General Comments, Questions

- Does this work include vendors and pharmaceutical companies that also want to get their hands on this data?
  - Policies surrounding all secondary uses of data – not just research and innovation but also performance measurement (PM) and quality improvement (QI). There may be a need for separate policies for these various initiatives.
  - What policies need to be put into place to ensure adequate capture of any economic benefit resulting from that data?

4. Explicit feedback references to Ministry PHIPA Modernization document





Slide #2

- Might be appropriate to highlight that all of these changes will also be underpinned by the need to protect PHI from misuse and inappropriate disclosure so as to ensure that trust in the system is maintained. It's implied but it has to be the starting point of any conversation around these issues.
- (virtual care) I would use the term Expanding the use of virtual care options....

Slide #3

- "Current framework does not allow ministry to truly monitor funding for public health care as delivered via Ontario Health Teams and elsewhere
  - I agree, but would make the direct call to say that financial information and social determinants need to be shared as part of any new operational model.
  - - to facilitate a move to a value based and integrated health system
  - - to help identify and optimize the gaps in care.

  We do not have any standards with regards to social determinants, (i.e. vulnerability index) so it's my opinion that should be called out.
- No regs indicating that the healthcare value-chain needs to be cyber/privacy compliant on both the technical and governance aspects of cybersecurity

Slide #4

- "If the patient gave consent, providers must share it."
  - Consider qualifying this with, "unless unreasonable or in violation of legal requirements", as there would be scenarios where this is not possible or where this conflicts with a provider's legal requirements.
- "Innovators and researchers would have access to de-identified health information to stimulate research, innovation, and economic development".
  - Clarify whether there's a de-identification standard to be used here, and if this is part of the recommendations.
  - Consider including transparency requirements
- Patients should be notified that such sharing will take place in all instances. Where the team members are in fact separate legal entities, an opportunity to opt-out of such sharing might be appropriate.
- I'm not sure the idea of allowing patients to get full access to their records from ANY health provider is a great idea... or would even work, as the ability for a small local office to have the staff or capacity to access my record from a more technologically complex organization will cause problems and confusion at the frontline... The patient should at any time be able to get their record from the place where it was captured
- Provider will be required to share PHI if the patient gave consent... I do think that consent directives need to be part of the process and accountabilities on the patient side...
- Ontario health teams... if these teams are acting as one entity then in my mind implied consent works across the entire team no different than today if you are getting services in a hospital that has multiple campuses... it's still one entity
- Researches have access today to de-identified health data via IC/ES but don't like it... how would this be different?
- (research and Innovation) aggregate?
- Must re-iterate that the value chain is cyber compliant from both technical and governance perspective
- Must ensure that this information when shared outside of ON both within Canada, US, EU and internationally are compliant with domestic and international cybersecurity and privacy requirements for the entire innovators/r&d value-chain. This is big data that has to be encrypted both at transit & rest

Slide #5

- "Reduce the time individuals must wait for an initial response to a formal access request"
  - Indicate the time range being requested (e.g., 5 days), and consider whether this is reasonable in practice across HICs of different records management maturity levels.
- "Establish a right to access Personal Health Information via a commonly accessible digital format."
  - Include a requirement for patients to provide opt-out consent for the use of data for secondary purposes.
- Critical for trust. It seems however that this point is less about reducing barriers to patient access than enabling innovation, which is a public policy objective that comes later on in the deck. I'd also suggest that the amendments require that reasonable measures be taken to ensure that PHI is de-identified and that any provider of de-identified data contractually prohibits downstream recipients from trying to re-identify the data.
- Fees... I thought that this had already been addressed? "reasonable cost recovery"
- I thought when hospitals fell under FOI that the same timelines had to be followed? Is this still an issue now that things like Epic MyChart are available... those results are in near real-time, unless abnormal results... Just not sure this is a real issue???
- Retention times certainly need to be clarified, especially if you will be allowed to go to any facility to gain access... if you are not the original collection facility, what is your obligation if you are just an access point... the data may still sit on your system in some way
- Creating/forcing a timeline where organizations must be able to provide information to requestors digitally would be a good thing... Just not sure that is the role of IPC
- New teeth in the legislation for those who knowingly or unknowingly re-identify data would be good
- (Need to ensure that the health teams can demonstrate that they undergo bi-annual cyber audits again from both technical and governance audits. Need to ensure that only those within organizations that need to access patient data have access to the critical data.
- Need to train patients on how to handle and share their data with the appropriate healthcare teams only. Not share their data on social media, etc.

Slide #6

- "Establish the privacy framework under which Ontario Health would be permitted to utilize Personal Health Information and to disclose Personal Health Information and de-identified data to Ontario Health Teams and other organizations."
  - Indicate who the "other organizations" are, by describing the type of organizations (e.g., other HICs, agencies, and researchers).
- "Enable Ontario Health Teams to share information for health care and planning purposes."
  - Clarify who the sharing would occur with and for what information.
- "Establish common interoperability standards." SA14
  - Clarify whether the legislation should indicate which standards to follow (e.g. HL7 FHIR), or the Province would put out policy to indicate the standards to follow, and/or certification against standards should be required.
- "(e.g. sharing Personal Health Information on emergency room readmissions across custodians)"
  - Clarify who are the targeted custodians in this recommendation.
- While these policy objectives are all sound, preference should be given to sharing of de-identified information over personally identifiable information, with the latter only being shared when necessary.
- I'm not sure how Ontario Health is any different than eHealth Ontario in this regard... their abilities are already described in the legislation... is this a name change?
- custodians already have the ability to use PHI for quality and planning purposes...?
- if custodians can already use their data to make improvements why would they need and prescribed registry or entity to give them back their own data... not sure having someone else data is helpful...? or needed?
- Must ensure that the entire health teams undergo cybersecurity governance training. Should request that the vendors and sub-contractors along the value chain can demonstrate that they qualify for at least $2M in cybersecurity insurance. Or else, insist the value-chain who is involved in data exchange undergo both technical and governance audits, education, pen testing, etc

SA14 Interoperability

We applaud the move to open APIs.

We believe that all organizations which create and use APIs must follow a certain set of minimum standards, and their implementation must be security and privacy reviewed and tested by a knowledgeable third party.

We have been deploying interoperability and data exchange solutions across our customer base for many years and currently have a deep library of interfaces which promote industry and international standards including HL7 (v2, v3, and FHIR), ANSI, EDI, and RESTful APIs as well as Integrating the Healthcare Enterprise (IHE) profiles for sharing patient data.

The creation of one unified EMR is perhaps unrealistic. Each EHR/EMR vendor has the same data, but it's often stored in different data elements. It would take significant time to accurately map all of those elements and combine it into one system. However, through the use of APIs this could certainly be achieved over time. But the question arises — who creates the central unified EMR? Who decides the layout of data structures? Who manages the infrastructure to house this vast database? Similar results can be achieved through the use of APIs in the near term, and could lay the basis for this future unified EMR.

Susan Anderson, 2020-02-06

Slide #7

- Since we are talking about disclosure of raw PHI to parties which are part of the circle of care, there should be obligations on the providers of data and the requestors/recipients of data to ensure that the principles of data minimization and proportionality are followed (ie do not request nor provide any more data than is strictly necessary to achieve a well defined purpose).
- this is important and I think could be expanded to enable interdepartmental... as school, corrections and social services continue to play a more important role, these actors should have the ability to share information
- I not sure this would really work... the example of the Coroner's office... they should focus on source systems for factual data, not secondary systems
- I don't agree as I have often had police fishing for information at health records... this puts undue risk on the custodian as people will get overprotective and potentially interfere with the provision of care
- health info custodians need to undergo both privacy and cyber governance education bi-annually. Ensure that their business continuity plan has cybersecurity governance policies in place, including BYOD, Vendor management policies.

Slide #8

- "Allow for the health card number to be used more broadly than for OHIP claims purposes."
  - Expand on this recommendation: is the intention for health card numbers to be used as digital health identifiers? What broader purposes are being contemplated?
- "Establish rules under PHIPA for the creation, use and sharing of de-identified data."
  - Should this be defined under the legislation, or a policy statement or guidance document? Would the IPC be the appropriate regulator in this case (regarding the use of de-identified data) and/or is there a role for the Patient Ombudsman?
- "Establish a review capability regarding the use of Personal Health Information or de-identified information for research / innovation purposes that benefit the public."
  - Who would be the regulatory/review body – the IPC, health care institutions' ethics review boards, and/or Ontario's Patient Ombudsman? Would an opt-out mechanism be required?
- **(health card # use)** Unsure what the purpose of this would be. Any unique identifier such as one's OHIP number is considered to be personal information, so that's one thing to keep in mind.
- **(creation of de-ident data)** It's appropriate for a privacy law to lay out the high-level criteria that must be met for PI/PHI to be considered de-identified (see comment on slide 5) . Once the data has been de-identified however, there should not be statutory rules around its "creation, use and sharing".
- not sure the use of the OHIP number fixes this problem... however having clear identifiers and identity would be good
- I'm not sure that PHIPA is the vehicle for this... I do think that if the government wants to drive innovation, they could use an organization like MARS to build out test databases that would be open to the public for use on innovation projects
- Need to ensure that encryption is utilized at both at rest & in transit. Need to ensure that when sharing this data outside of ON both domestically and internationally that the means in sharing this information is compliant with the various regulations both found within Canada and internationally.
- there should be a bullet point about chain of custody of any non aggregated information and PHI such as a health card number. all access needs to be journaled and only accessible through a credentialed system to prevent unauthorized access.

Slide #9

- "Allow for improved tracking of publicly funded health care."
  - Clarify what's meant by "tracking": What type of data is the objective for this tracking recommendation (e.g., data utilization, visits, health outcomes, spending and budgets, etc.)?
- "Authorize a unit of the Ministry of Health…"
  - Is this intended to be part of an existing unit in the Ministry of Health? Would this require the creation of single unit at the Ministry of Health or multiple units across the Province (e.g., multiple data integration unit(s) which may be set up across the OPS)? Would HICs establish and run these integration units (with their service providers), or would these be developed and run by the Ministry?
- "Create the ability for integrated data to be available to researchers for analysis…"
  - Indicate the types of potential researchers. For example, would this include any type of researcher (publicly-funded, private, etc.)?
  - What is the targeted 'integrated data', and would this data be de-identified or potentially identifiable?
- agree that the gov should track the healthcare spend but not sure that requires PHI
- I don't understand gov role in research... I do agree that gov should have access to all data for any system improvement, not just to hospital but public health and social programs... I don't think this has to be PHI... as for research there is a good path and other tools/venues for them to get the information... the reality (in my mind) is that research is the monetization of data... for cash, publications or recognition... it is still data being monetized for some reason... I'm not sure that gov has a role in this... unless they are actually looking at monetizing their population data... which I think is a different topic all together...
- Need to ensure that the ministry and the health data custodians undergo audits both from technical and governance perspective and address the gaps at least on bi-annual basis

Slide #10

- **(government tracking of healthcare funding)** I assume we're talking about de-identified data here, correct? It seems PHI is not needed for this purpose...
- **(government health data use)** This reminds me a bit of the Stats Can story from earlier this year, where the agency tried to obtain banking information from a sample of Canadians from the banks, which Stats Can was going to anonymize themselves for analysis. This created a major backlash, as Canadians did not trust a government agency to appropriately use and protect/secure/their data.I can see a similar risk here as well. To the extent there is another way of achieving the same purpose (e.g. require providers to de-identify the dataset before providing it to the ministry of health), it should be the preferred approach.
- (**patient**) adding a third bullet: Ontarians will have access to a continuum of care; virtual and/or in person.
- (**patient**) adding a third bullet: Ontarians will have access to a continuum of care; virtual and/or in person.
- patients should be accessing this data in an encrypted environment. info should be shared in a virtual machine
- best practices to manage patient communication & health team communication not email all vendors/sub-contractors along the health team need to display they are privacy and cyber compliant- qualify for $2M in cybersecurity insurance- undergo audits, education for entire organization, pen testing, ensure encryption in play, only give access to certain health data custodian and then remove access to those who no longer work or left the organization from accessing patient data, non-disclosure/confidentiality agreements should be in place each time both patient and health team custodian accesses data, ensure policies in place for storage, retention and delivery of the health data, have policies in place for breach notification responsibilities, must have right to audit policies in place, ensure vendors/sub-contractors have limited patient data limitations and policies in place; ensure that both sub-contractors and vendor obligation policies in place for termination of access of patient data upon completion of access

Bibliography

CLICK TO ADD SUBTITLE

Bibliography of Relevant Documents

1. comments of the IPC Ontario on Bill 128 by Ontario's Office of Privacy Commissioner
2. ITAC Health Letter to the Editor of Globe and Mail, November, 2019
3. ITAC Health Strategy Document for 2019-2021
4. CIHI's 2013 Health System Use Vision Report to the FPT Deputy Ministers on Health System Use
5. David Naylor Panel July 2015 Innovation Report to Health Canada
6. Digital Health Canada CHIEF White Paper on 'Unlocking the Value of Data'
7. **ITAC Health Submission to Advisory Panel on Healthcare Innovation – Advancing Health and Prosperity**
8. **ITAC Health Interoperability and Standards Committee (ISC) Position on Canadian Healthcare Interoperability Standards** – *November 14, 2016*
9. **ITAC Health White Paper**: **Accelerating the Adoption of Digital Health Technologies in Canada** – *October 2018*
10. **"Research ethics: are we minimizing harm or maximizing bureaucracy?" ;** KAREN ROBSON & REANA MAIER | OCT 08 2018; https://www.universityaffairs.ca/opinion/in-my-opinion/research-ethics-are-we-minimizing-harm-or-maximizing-bureaucracy/