

INQ

2023
PHIA Review
Final Report

OCTOBER, 2023

TABLE OF CONTENTS

Glossary	3
Executive Summary	4
The PHIA Review Committee	6
Principles for the PHIA Review	8
Environmental Scan – SnapShot	9
Consultations – What We Heard	10
Provincial Consultation	10
Canadian Consultations	11
Written Submissions Summary	12
Survey Summary	12
Methodology and Approach	12
Overview of Participants	13
Key Observations	14
Survey Summary Analysis	16
Key Recommendations	17
Privacy Protections	17
Access to Health Data & Interoperability	21
Data & Innovation	24
Monitoring & Oversight	28
Consent	30
Literacy & Social License	34
Other	37
Prior PHIA Review (Rollover Recommendations)	40
Conclusion	41
References	42
Appendix A: Current Legislative Landscape	
Health Privacy Laws of Canada	43

GLOSSARY

Please refer to the [Personal Health Information Act](#) for additional definitions.

Collection: In relation to personal health information (PHI): where a custodian gathers, acquires or obtains the information by any means from any source.

Consent: Consent refers to the ability to give free, specific and informed agreement to the sharing of PHI. Please refer to PHIA for definition.

Custodian: an individual or an organization who has custody and/or control of PHI, and who has accountability for the protection of PHI, as defined in PHIA.

Disclosure: Disclosure, in relation to PHI in the custody or control of a custodian or other person, means to make the information available or to release it, but it does not include use of the information.

Interoperability: refers to the ability for information to flow seamlessly between different solutions and devices. When different parts of the health system are interoperable with each other, they can “speak the same language.”

Legislation: a law or laws, and for the purposes of this paper, includes associated regulations.

NL: Newfoundland & Labrador.

Personal health information (PHI): information that relates to an individual’s health status and can identify that individual either on its own or in reasonable combination with other information. Please refer to PHIA for definition.

PHIA: Personal Health Information Act, NL

Virtual care: any interaction between patients and/or members of their circle of care, occurring remotely, using any forms of communication or information technologies, with the aim of facilitating or maximizing the quality and effectiveness of patient care.

Virtual care solution: the means by which virtual care is provided. Generally, a solution in this context refers to technology.

EXECUTIVE SUMMARY

Proclaimed in 2011, the *Personal Health Information Act* (PHIA, or the “Act”) is required to undergo a review once every five years. The Act establishes rules that custodians of personal health information must follow when collecting, using, and/or disclosing individuals’ personal health information.

The province engaged INQ Consulting to complete a statutory review of PHIA. A statutory review committee (the “Committee”) was established with representatives from INQ Consulting and officials from the Department of Health and Community Services (see the PHIA Review Committee below for members).

The purpose of the review was to assess whether there should be changes to modernize PHIA. The review was undertaken in three key phases as outlined below:

1

LITERATURE & LEGAL REVIEW

Environmental scan looking at opportunities for improvement & legislation from other jurisdictions.

2

CONSULTATION

Up to 15 interviews across NL and country (Provincial stakeholders, Federal entities, etc.)

3

IMPLEMENTATION PLAN & REPORT

Recommendations to modernize legislation.

The Committee consulted a broad range of stakeholders to ensure various perspectives were duly considered with over fifteen consultation sessions. Stakeholders included, among others, members of the general public, Indigenous groups, patient councils, government departments & agencies in the province, and regulatory bodies. The Committee gathered information and opinions in a systematic manner that allowed stakeholders and individuals to bring forth the issues that mattered to them through the collection of nine written submissions, as well as two hundred and eighty-three survey responses.

This PHIA review lays a foundation for additional and potentially significant reforms to PHIA, particularly with the advancement of Federal Bill C-27 (pending) and the rapid advancement of artificial intelligence (AI) in healthcare. Specifically, the Committee expects that PHIA will need to undergo a series of amendments in order to maintain its “substantially similar” status with the federal Personal Information Protection and Electronic Documents Act (“PIPEDA”). Currently, PHIA is considered “substantially similar” to PIPEDA as it:

- provides equal privacy protection
- contains the 10 PIPEDA fair information principles

- provides for independent oversight and redress with the power to investigate
- allows the collection, use and disclosure of personal information only for appropriate or legitimate purposes

Therefore, the recommendations put forward by the Committee include those that are of high priority at this time, while taking into account the future anticipated changes that may stem from Bill C-27, if passed into law. To this end, the Committee has avoided tabling recommendations that could either be duplicative or require an extensive overhaul if Bill C-27 is passed. For example, while the Committee acknowledges the importance of regulating AI, this report does not make radical changes that deviate from potential future amendments in Newfoundland and Labrador (NL) should Bill C-27 become law. While the Committee makes no claim on exactly what the final content of Bill C-27 might be if passed into law, this review and resulting recommendations aim to support a more comprehensive regulatory regime for AI. Finally, this report includes recommendations from the 2017 PHIA Review that remain current and of importance for this province.

On the whole, this report makes recommendations about the interpretation of roles and custodianship, the development of a

data stewardship council, Indigenous data sovereignty and various other key recommendations to modernize the Act. Overall, these changes reflect modern data values and practices that protect privacy, strengthen individual rights to their own personal health information, and enable greater innovation in the health sector.

Readers will find in the report direct committee observations or quotations from our consultation sessions, as well as references from written submissions. While these observations do not always correspond to recommendations, they constitute a genuine effort to reflect our engagement with stakeholders who have taken the time to inform the review. Written submissions and feedback referenced in this report may be contained either directly within this report or on the PHIA Review (2023) website, found online:

<https://www.phiareviewnl.ca/publications>

The province of NL is in a unique position to leverage over a decade of experience with PHIA, implement learnings from the recent cyber-attack, as well as take advantage of opportunities to advance a modern privacy approach in a digitally connected world.

PHIA Review Committee

The PHIA Review Committee included members of the INQ team (below) and the following representatives from the Department of Health and Community Services, Government of NL:

1. Justin Caines, Legislative Consultant
2. Donna Roche, Director Data Governance and Privacy
3. Stefan Brunet, Regulatory Development Consultant
4. Kimberly Ryan, Manager of Privacy and Information Security

The INQ Team

INQ is a firm of intensely curious and knowledgeable lawyers and consultants. Our collective experiences and expertise guide clients through some of their most complex challenges. We are committed to providing common sense solutions, while staying on top of emerging trends to help our clients thrive.

INQ was founded with a focus on privacy, data governance, cybersecurity, and AI. INQ combines our established reputations as leaders in health law, data law and corporate law, as well as offering its clients an integrated, thoughtful, and dynamic consulting services to take clients from idea to implementation in any sector.



Angela Power

Senior Director, Ethicist, INQ Consulting

Angela is an ethicist who brings practical and strategic advice to assist organizations with privacy, data governance, & ethics, particularly for digital health, AI & other emerging technologies.



David Goodis

Advisor, INQ Consulting

With more than 30 years of experience, David was the Assistant Information and Privacy Commissioner of Ontario and has deep expertise in the application and enforcement of privacy and access laws.



Carole Piovesan

Co-founder & Principal, INQ Consulting

Carole focuses her practice on privacy, cyber readiness, data governance and artificial intelligence (AI) risk management. She plays an active role in shaping data law, policy and standards in Canada and globally.



Samara Starkman

Co-founder & Managing Principal, INQ Consulting

Samara brings both practical and strategic advice to assist organizations with responsible, compliant innovation. Prior to INQ, she ran a consulting firm advising clients including major Ontario hospitals & pharmaceutical companies.

Principles for the PHIA Review

The following principles were established at the outset of the review as key objectives to accomplish. These principles were communicated at the outset of all consultation sessions, in all PHIA review materials and any preparatory materials provided to stakeholders prior to engagement.

1	Maximize benefits for patients.
2	Ensure patient access to their own information is paramount.
3	Enable choice and modern consent so that patients can have their own information flow where, when and to whom they desire (in a timely fashion).
4	Consider concepts of sound data governance and stewardship.
5	Reduce silos.
6	Foster collaboration and partnerships in line with patient desires and choices.
7	Transparency and accountability is key.
8	Foster data literacy and autonomous choice.
9	Patients benefit when their PHI is protected and only shared to those who they wish to share it with and those who are authorized to access.
10	Patients benefit from health data sharing among their providers.
11	Patients benefit from having increased control over their health data.
12	Increased collaboration across sites & jurisdictions is desirable because it benefits all Newfoundland & Labradoreans.
13	There is a benefit to aligning NL practices with those of other provinces and, in some cases, beyond Canada, i.e., European Union's General Data Protection Regulation (GDPR).

ENVIRONMENTAL SCAN – SNAPSHOT

The Environmental Scan was conducted as Phase 1 of the PHIA Review and was undertaken to understand the health privacy landscape in both Canada and internationally. Key learnings have been embedded into this final report and recommendations.

There are increasing demands for health data, including PHI, to support and sustain the health innovation sector. For instance, AI and other digital health technologies are experiencing exponential growth. AI is being considered across clinical practice, biomedical research, public health and health administration. AI requires a new policy and regulatory approach. In response, Bill C-27 has proposed a new federal act to reflect the rise in AI and ensure there are legal requirements for AI systems.

One of the trends observed include an increasing demand for the custodian model to be replaced by the stewardship model, which is a paradigm shift away from a culture of caution and gatekeeping of data that is perceived by some to be a major challenge in Canada, towards a culture whereby data sharing is supported and advanced according to laws and ethics. What this exactly means for PHIA and other health privacy statutes is not entirely clear, however the concept of “data stewardship” is represented as a theme arising from this review and an area of potential opportunity moving forward.

Another observation includes growing concerns regarding custodians' understanding of their legal obligations that results in a ‘culture of caution’ when interpreting rules. There are also calls for action to improve the general public’s data literacy, which is needed to understand the changes to health privacy legislation today and in the future. Finally, de-identification has emerged into legislation with greater specificity and a sense of urgency.

Overall, the key findings include:

Develop flexible frameworks so the legislation can adapt to technical innovations.

Increase public confidence and public awareness.

Increase awareness and education to smaller private custodians.

Strengthen influence of Commissioners through fines and penalties.

Increase privacy protections through mandatory breach reporting and PIAs.

CONSULTATIONS – WHAT WE HEARD

One or more consultation sessions took place throughout 2022-23 with the following stakeholders:

Provincial Consultation

1	Patient Council Members (Patient Representatives)
2	Office of the Information & Privacy Commissioner (OIPC), NL
3	Newfoundland & Labrador Medical Association (NLMA)
4	Digital Health Division, Department of Health and Community Services
5	Policy Division, Department of Health and Community Services
6	Nunatsiavut Government
7	Newfoundland & Labrador Centre for Health Information
8	Newfoundland & Labrador Health Services (NLHS)
9	Memorial University
10	Digital Government and Service NL
11	Canadian Institute of Health Information (CIHI)

“And the thing is life is in the gray areas. And as a human being, you can pick up the subtle differences or think of different ways of doing things ...I'm not sure that AI is there yet.”

Member of the General Public

Canadian Consultations

The below consultations took place throughout the Winter and Spring, 2023.

1	Government of Canada (on Bill C-27)
2	Government of Quebec (on Bill 3)
3	Government of Ontario (on PHIPA)
4	Government of British Columbia (on PIPA)
5	Government of Alberta (on HIA)

With recent virtual care advancements in health and broad digital health transformation, there are more opportunities to access and share patients' PHI. Canadian jurisdictions are beginning to better reflect these digital advancements in their legislation in an attempt to modernize access and privacy laws. Common recent amendments across Canada focus on consent, digital health requirements, fines, electronic access to PHI, research and notice. Ontario is also "considering proposals that would implement a fundamental right to privacy for Ontarians, introduce more safeguards for AI technologies, introduce dedicated protections for children, update consent rules to reflect the modern data economy, promote responsible innovation and correct the systemic power imbalances that have emerged between individuals and organizations that collect and use their data."²

Notably, within British Columbia, there is a Data Stewardship Committee (DSC) established under the E-Health (Personal Health Information Access and Protection of Privacy Act). The (DSC) prioritized consideration of requests for data access, including for PharmaNet data and research related to declared Public Health Emergencies. Notably, "the committee members are appointed by the Minister of Health, and are responsible for managing the disclosure of information contained in a health information bank or a prescribed MoH database."³

The DSC is made up of physicians, leading researchers, among others. Overtime, it has become difficult to determine whether a research project violates the clause that prohibits market research, which is also a relevant topic for NL as the future of data governance is being considered.

Within Alberta it was reported that there are increasing demands for health data for research and other purposes, including commercial uses. These expanded uses continue to strain policy directives and resources under the *Alberta Health Information Act*⁴ ("HIA").

WRITTEN SUBMISSIONS SUMMARY

The Committee received written submissions from the following groups:

- Members of the General Public
- Office of the Information and Privacy Commissioner, NL
- Newfoundland and Labrador Medical Association
- The Canadian Medical Protective Association
- The Adult Protection Program of the Department of Children, Seniors and Social Development, Government of Newfoundland and Labrador
- Newfoundland and Labrador Centre for Health Information
- Western Health
- Workplace NL
- eDOCSNL Program

SURVEY SUMMARY

The Department of Health and Community Services (HCS) sought feedback to understand the public's opinions, viewpoints, and concerns about the review of the PHIA, as well as health privacy, collection, use, disclosure and general protection of personal health information.

The survey/review:

- solicited insights on the public's perceptions and concerns about privacy, their health data and how information is protected by custodians in the province.
- gathered input and feedback to ensure that the Act serves the needs of the public, that it is functioning as it should and that any necessary amendments are contemplated in a timely fashion.

Input from the engagement and consultation process has been used to inform legislative amendments to the PHIA.

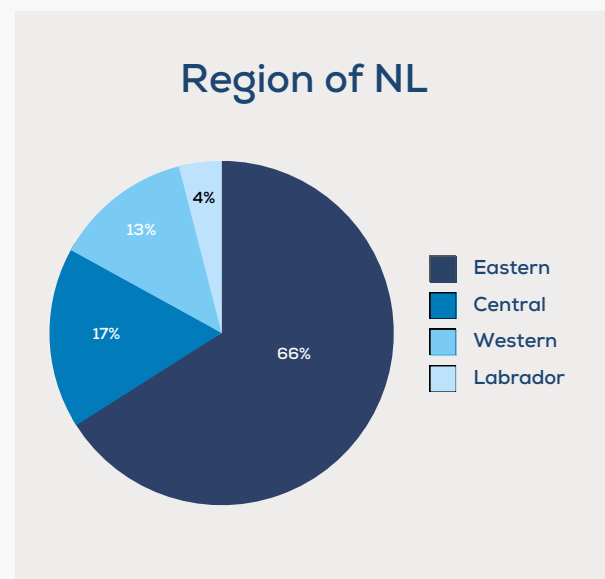
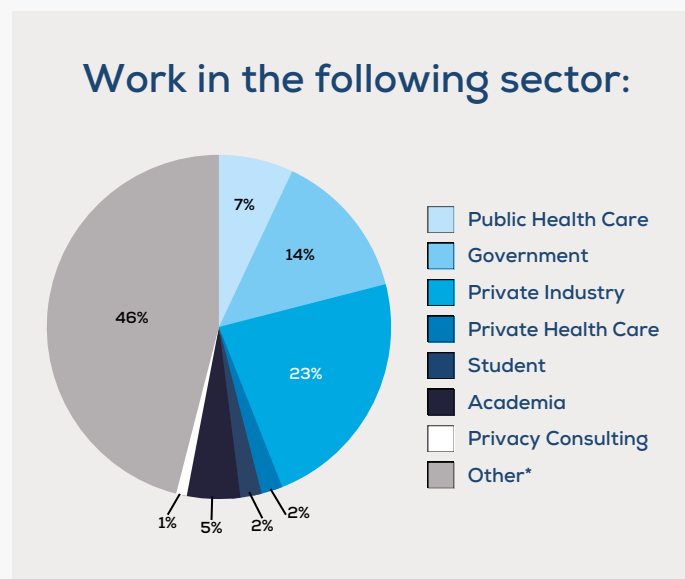
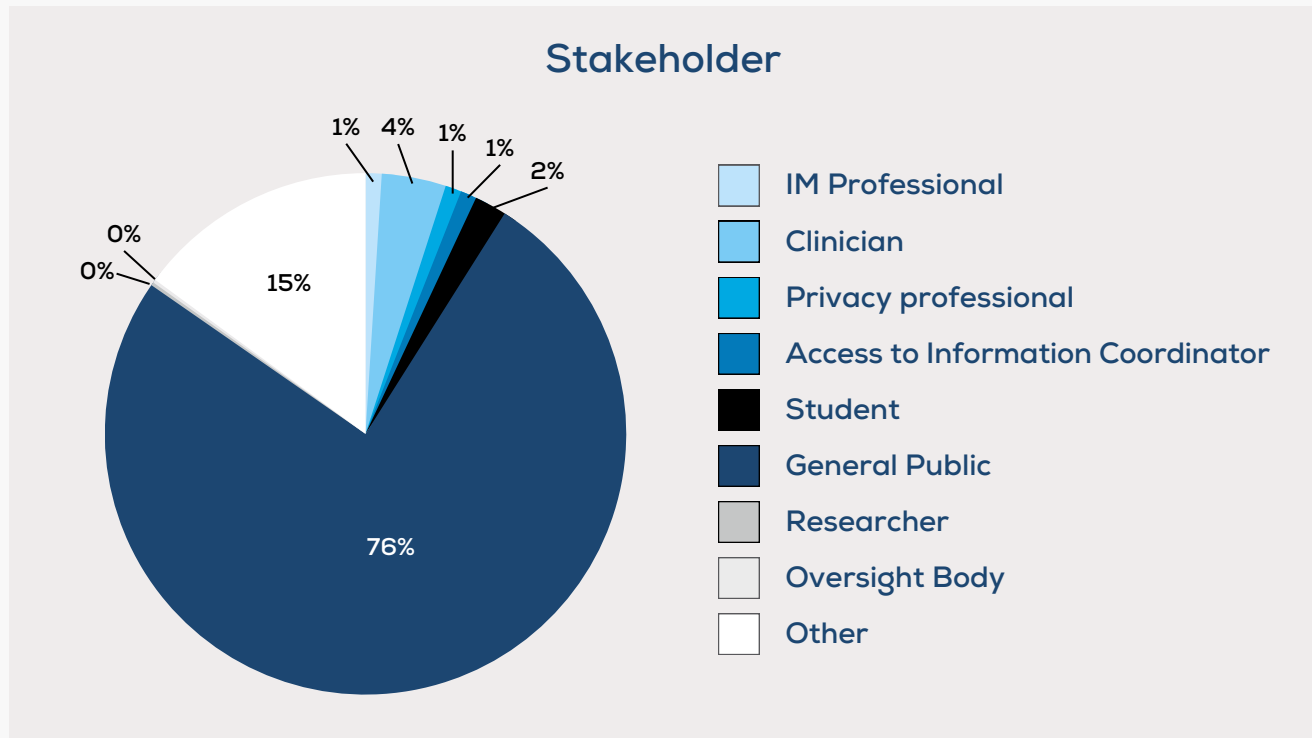
Methodology and Approach

The approach utilized to gather input into the PHIA Review 2023 included the development of a landing page and online questionnaire posted to the engageNL platform from May 3-24, 2023.

The landing page on engageNL included an email address linked to the department where individuals could provide written submissions.

Overview of Participants

Two hundred and eighty-three participants completed the online questionnaire during the engagement process. Respondents were asked demographic questions to identify the stakeholder group, which sector they work in, and region in which they live. 76% identified as the general public. For a further breakdown of participants by percentage is provided in the charts below.



***NOTE:** 46% of respondents identified 'other' as their selection. A review of the data showed the majority of respondents identified that they are retired.

Key Observations

Some of the key findings resulting from the questionnaire are outlined below.

Participants were asked statements regarding awareness of the *Personal Health Information Act* (PHIA). Below are some of the statements included in the engageNL questionnaire and participants' responses. **Note:** The graph that follows also highlights these findings.

I am aware that there is a Personal Health Information Act (PHIA) in the province that provides patients with privacy and access rights.

88% of respondents (249 respondents) indicated they were aware that there is an Act (PHIA) in the province that provides patients with privacy and access rights.

I am aware I can request my personal health information under PHIA.

72% of respondents (203 respondents) were aware they could request personal health information (PHI) under PHIA.

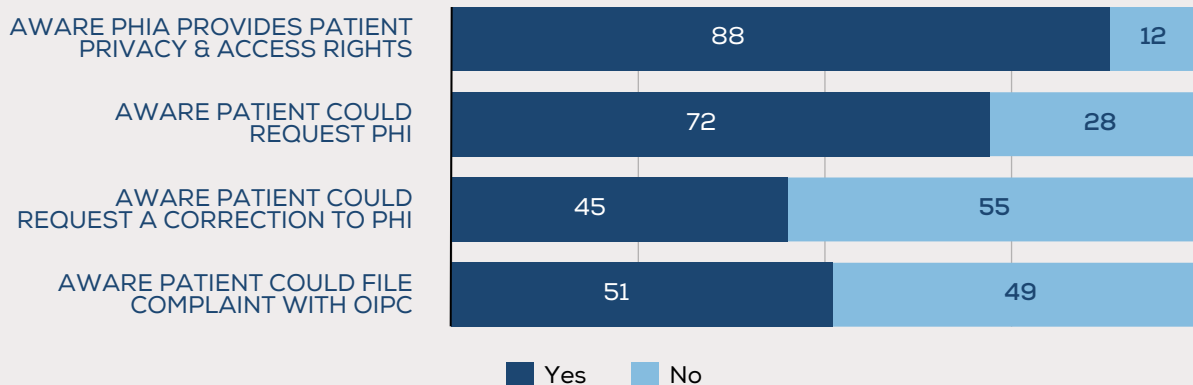
I am aware I can request a correction of my personal health information under PHIA.

45% of respondents (128 respondents) were aware they could request a correction of their personal health information under PHIA.

I am aware I can file a complaint with the Office of the Information and Privacy Commissioner (OIPC) under PHIA for denial by a custodian of a request for access or correction to my personal health information.

51% of respondents (144 respondents) were aware they could file a complaint with the Office of the Information and Privacy Commissioner (OIPC) under PHIA for denial by a custodian of a request for access or correction to their personal health information. All respondents that were aware they could file a complaint with OIPC indicated they had not filed a complaint.

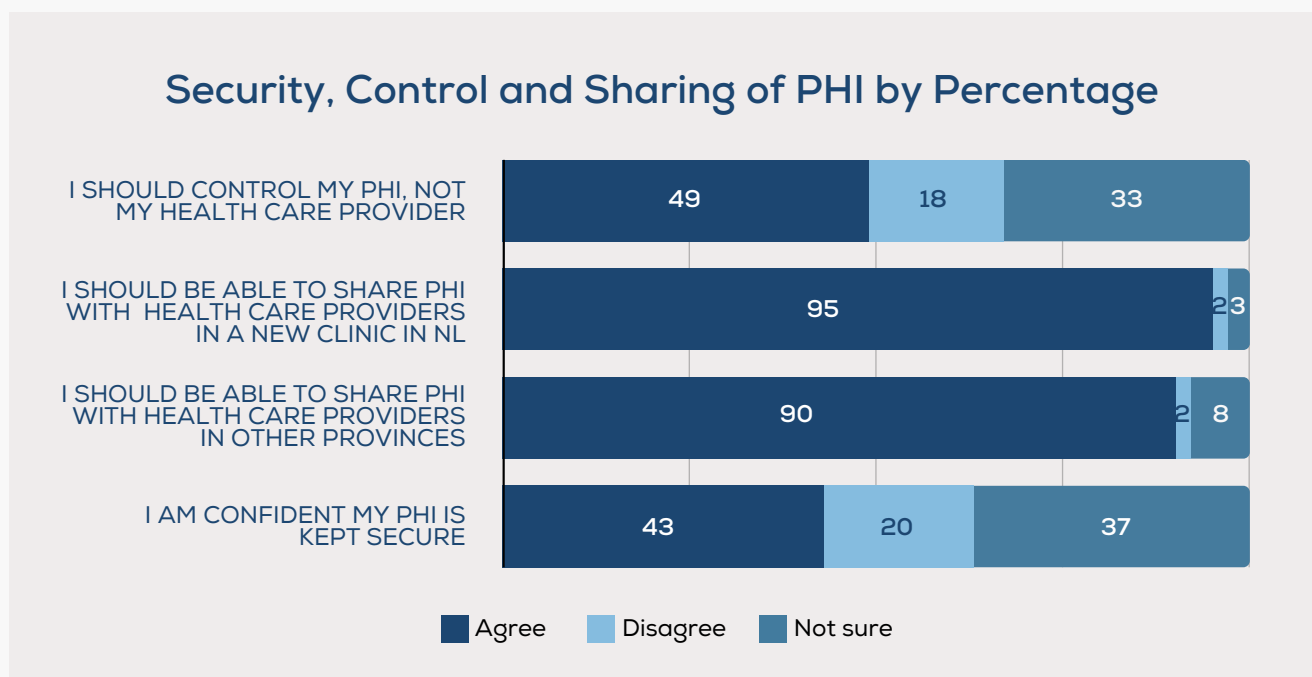
Personal Health Information Act Awareness by Percentage



The chart below indicates how respondents felt about how secure their personal health information was, who should control their personal health information and with whom they should be able to share their personal health information.

The statements asked included:

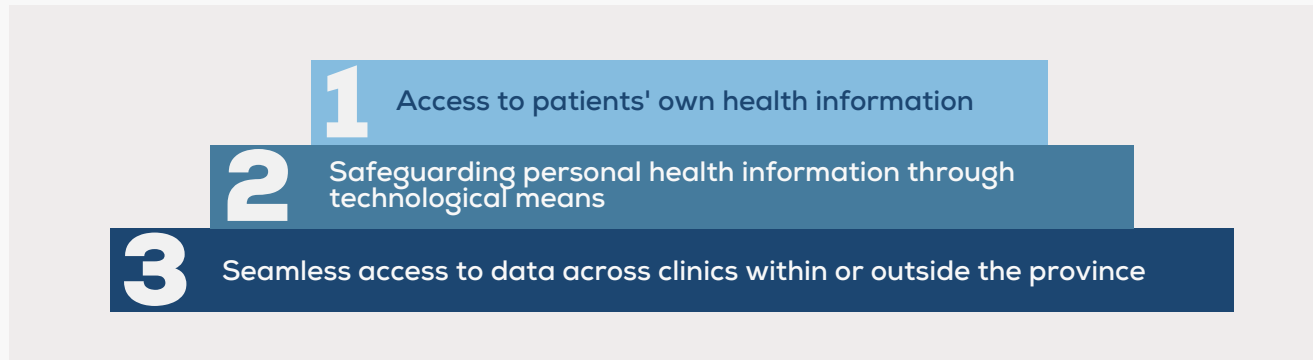
- I should control my personal health information, not my healthcare providers.
- I should be able to easily share my personal health information with health care providers in a new clinic for care within the province.
- I should be able to easily share my personal health information with health care providers in other provinces for care.
- Overall, I am confident my personal health information is kept secure.



Respondents were asked “ In your opinion, what are the top 3 areas that the PHIA review should focus on?” and provided with the following options in a drop down list:

- Providing consent for using and sharing your personal health information
- Access to patients’ own personal health information
- Research, including genetic research, using personal health information
- Safeguarding personal health information through technological means
- Privacy breaches or unauthorized access, use or sharing of personal health information
- Sanctions or fines relating to privacy breaches of personal health information
- Seamless access to data across clinics within or outside the province
- Special privacy and access considerations for digital health, artificial intelligence or other emerging technologies
- Other

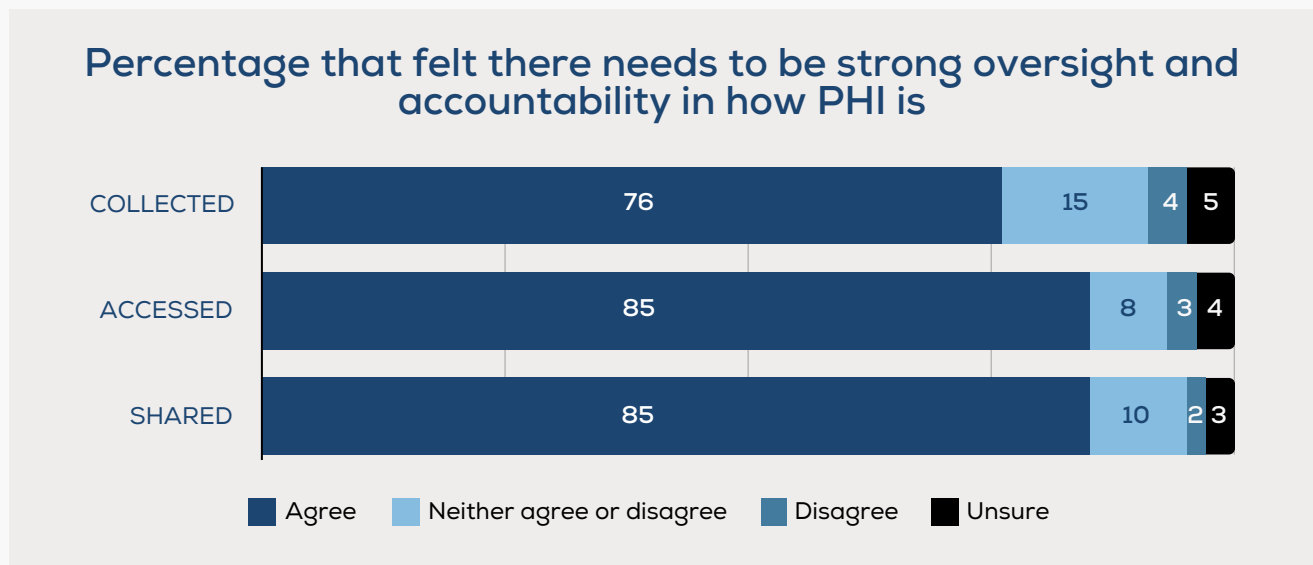
The chart below highlights the top three selections with one being the highest priority identified.



The chart below highlights how respondents felt about the oversight and accountability of how personal health information is collected, accessed and shared.

The statements asked included:

- There needs to be stronger oversight and accountability in how personal health information is: **COLLECTED**
- There needs to be stronger oversight and accountability in how personal health information is: **ACCESSED**
- There needs to be stronger oversight and accountability in how personal health information is: **SHARED**



Survey Summary Analysis

Participants expressed that the public should have more information about how personal health data is accessed and shared. They felt there was a lack of information on the subject and more public education needed.

KEY RECOMMENDATIONS

Privacy Protections

Upholding privacy protections is of utmost importance. Within NL there were many issues raised with respect to privacy, namely challenges related to:

- the interpretation and issue of simultaneous custodians,
- handling of data for research purposes,
- how Memorial University and its faculties are characterized under the Act,
- cross-jurisdictional breaches and incidents. In particular, the extent to which an individual can seek redress if their information has moved to another jurisdiction, and they are the victim of a privacy breach.

“And the big issue is, when you go... to a physician or to a health facility, you want to make sure that they got your information, but you don't want anybody to be able to, [go into] your system and get your information. You want the right people to have it but not the wrong.”

Member of the General Public

Ensuring Accountability & Clarity of Roles

RATIONALE

There have been ongoing challenges in the province with ensuring clarity on roles and ultimately who is the custodian or entity that should be responsible for safeguarding personal health information when there are two entities using the same PHI. According to the OIPC, "Attention should be given to identifying circumstances that can arise where there may be confusion about which of two or more parties is the custodian. This may include situations where multiple health organizations may both be involved in handling the same information – they cannot all be custodians of the same instance of the same information. Shared custodianship undermines accountability."⁵ Additionally, privacy management programs have become standard practice to enable adherence to the requirements under privacy legislation, including the proposed Bill C-27.

RECOMMENDATION

- a) Update section 4 of PHIA to ensure the operators of a facility, pharmacy, service centre, program, or group practice are identified as the custodian, and not health care professionals or health care providers reporting to operators.
- b) Add the affiliate (from AB) or agent (from ON) role to clarify roles of multiple parties. Include ability to update PHIA Regulations to include an updated list of affiliates/agents overtime OR ensure that provision exists to allow for agreement between the parties by contractual means. For instance, physicians can be affiliates of the hospital in which they work, which can be agreed upon by contract. However, if the physician rents space in a hospital and is not working on behalf of the hospital, then they would be a custodian.
- c) Include in the Regulations that operators of a group practice (a term that should be defined in PHIA) act as the custodian; with all other parties acting as affiliates. Where the group practice is an equal partnership amongst many providers, update PHIA to require one to be named as the contact person under s.18 of the Act.
- d) Change current affiliation agreement in regs and expand to include other trainees who are not healthcare professionals (i.e., clerk/administrator).
- e) PHIA is applicable to anyone with a defined legislative authority to collect, use, and/or disclose PHI in accordance with the roles established in the Act. Ensure all necessary roles are defined and are included in the Act.
- f) Mandate that anyone defined as falling within the scope of PHIA's application must have a privacy management program in place that aligns with the proposed Bill C-27.

Privacy Protections Recommendation 2

Memorial University & Research

RATIONALE

Although universities and specific faculties and researchers on the whole are not considered custodians in other jurisdictions, since PHIA came into force in 2011, the Faculty of Medicine, the School of Nursing, the School of Pharmacy, and the School of Human Kinetics and Recreation, have all been custodians in accordance with section 4(1)(j). Memorial University has expressed a desire to align with other jurisdictions, specifically that they should not be custodians. Other stakeholders in the province seek to ensure that faculty members and students who have PHI in their control or custody maintain privacy protections and believe the way to do so is to maintain status quo with the faculties named in PHIA.

Finally, the process of registry designation is not contained within the Act or Regulations and lacks clarity in terms of how and when registries may be sanctioned appropriately and have ongoing annual approvals.

RECOMMENDATION

- a) Add provisions that require an agreement with custodians when sharing PHI with researchers that will bind researchers to PHIA and ensure adequate protections for PHI in the research context.
- b) Add a provision to include sharing of PHI to/from researchers and custodians ensure that anyone holding data as, or on behalf of, a researcher, must comply with the provisions of PHIA as if they are a custodian (refer to s.54 of Alberta's HIA).
- c) Add 'registry designation' processes and criteria, including ongoing oversight and approval processes, to the Act or Regulations. This will ensure clarity of roles and responsibilities for sanctioned 'Registries' of PHI that are managed within the province.
- d) Add research (Research Ethics Board) provisions for ethics approval/evaluation, similar to what is found in s. 50 of Alberta's HIA.
- e) Given above adequate protections that align to other jurisdictions, remove Memorial University's listed faculties as custodians under the Act.

Privacy Protections Recommendation 3

Cyber Requirements

RATIONALE

NL experienced a cyber-attack that was deemed the largest privacy breach ever experienced in this province, which saw the personal health information or personal information of the vast majority of our population taken by malicious threat actors. It was also one of the largest ransomware attacks in Canada to date.

Throughout consultations with stakeholders across the province, it was clear that many custodians are unaware of what constitutes reasonable security protections and security measures, particularly as it relates to cyber security vulnerabilities.

Privacy laws across Canada have not provided prescriptive rules on cyber security, but rather have taken a high-level approach to signify the need for reasonable protections for security. The Federal government has sought to codify cybersecurity obligations in legislation of late with Bill C-26 - *Critical Cyber Systems Protections Act* (CCSPA).

RECOMMENDATION

a) Expand s. 15 of the Act to include the provisions of reasonable measures that align to national and international cyber security standards.

Access to Health Data & Interoperability

The digital era has increased demand for individuals accessing their PHI and allowing for the safe sharing of information to better inform decision-making for care. Supporting patient autonomy over their own information is critical, as well as ensuring individuals have direct access to their own information. This is consistent with the direction that most jurisdictions are going as far as emerging digital health technologies and the implementation of a Patient Health Record (PHR). The PHR and other efforts may support individual access to their PHI. It may also enable patients to drive and promote access to their information where they see benefit to either themselves, their families, or communities at large.

The key is recognizing the imperative of upholding privacy obligations, while at the same time maximizing benefits of sharing information, where appropriate. Individuals are demanding to have clear and manageable access to their personal information or data and want to be free to share or transfer it without undue burden.

“Custodianship models in Canada were designed when records were in paper or in health information systems in hospitals, where it was clear who was responsible for the records. Health information was not easily shared digitally between custodians, and custodians did not have shared interest in the accountability for the personal health information. In the last 15 years the landscape has changed significantly”

NLMA Submission

Remove Undue Burden to Access PHI

RATIONALE

Patients in the province have expressed concern that they are experiencing challenges accessing their own PHI.

There also continue to be challenges enabling interoperability and a general lack of knowledge amongst custodians on what is required to enable sharing between providers or across interoperable solutions for the purpose of care.

RECOMMENDATION

- a) To the extent that there is ambiguity in its interpretation or its application, the Act should be interpreted in a manner that treats the individuals' right to make decisions about their own information as prevailing.
- b) Add to the purpose of the Act that it is intended to uphold the right of individuals to have the requisite knowledge and ability to decide for themselves who gets access to their PHI.
- c) As with all jurisdictions across Canada, NL should move forward to have interoperable systems that enable sharing of PHI as a goal and mandate that interoperable systems be selected or built whenever possible.

Access to Health Data & Interoperability Recommendation 2

Circle of Care Clarified

RATIONALE

There continues to be ambiguity over sharing PHI using implied consent within the circle of care, particularly for unnamed custodians.

RECOMMENDATION

- a) Remove the current meaning of 'circle of care' in s. 24(3) and add a definition of "Circle of Care" in the Act (s. 2) in order to provide greater clarity.
- b) Add greater specificity to the Regulations on criteria when contemplating which custodian is in the circle of care. Ensure that custodians that are currently having difficulty obtaining PHI using implied consent when they are in the circle of care, such as cases reported with family physicians, Nunatsiavut government, and out of province professionals/providers, are considered.

Access to Health Data & Interoperability Recommendation 3

Education Campaign on Access Rights

RATIONALE

Patients expressed that they believe many individuals in the province are unaware that they have rights to access their own PHI. It was also believed that access rights were not well understood by all custodians, particularly by smaller custodians who may not be accustomed to receiving such requests.

RECOMMENDATION

Create a communications / education campaign to ensure that the concept of 'circle of care' is understood and that custodians consider the individuals' desires/wishes such that there are no unnecessary burdens applied for PHI to flow appropriately and securely.

Data & Innovation

With emerging technologies in health, legislation needs to facilitate innovation in a responsible way. Virtual care, AI and other emerging health innovations have the capacity to radically improve and respond to the growing pressures with our health system.

New technologies can improve the health of patients, families, and communities; however, they come with recognized risks and potential harms that will need to be effectively managed.

“In June 2022, the Government of Canada tabled the Artificial Intelligence and Data Act (AIDA) as part of Bill C-27, the Digital Charter Implementation Act, 2022. The AIDA represents an important milestone in implementing the Digital Charter and ensuring that Canadians can trust the digital technologies that they use every day. The design, development, and use of AI systems must be safe, and must respect the values of Canadians. The framework proposed in the AIDA is the first step towards a new regulatory system designed to guide AI innovation in a positive direction, and to encourage the responsible adoption of AI technologies.” (The Artificial Intelligence and Data Act (AIDA) – Companion document)

Overall, Bill C-27 Bill would not only modify PIPEDA, but would also implement three new laws:

- The Consumer Privacy Protection Act ('CPPA'), which is the privacy law that will replace PIPEDA.
- The Personal Information and Data Protection Tribunal Act, which would create a new Personal Information and Data Protection Tribunal ('the Tribunal') to review the findings of the Office of the Privacy Commissioner of Canada ('OPC') and levy penalties.
- The Artificial Intelligence and Data Act ('the AI Act'), which is framework legislation that would prohibit certain conduct in relation to AI systems that may result in serious harm to individuals or their interests. The full impact of the legislation is not yet clear as much of the detail has been left to regulations, which are not yet drafted.

The below table outlines the pending regulatory regime and key takeaways for Bill C-27 in Canada to govern AI:

Key Requirements	AI Management Program	Oversight	Penalties
<ul style="list-style-type: none"> AI legal requirements for users of "high-impact" AI systems AI and Data Commissioner; Ministerial powers Penalties Offences and criminal liability 	<p>AI legal requirements for users of "high-impact" AI systems:</p> <ul style="list-style-type: none"> establish measures to manage anonymized data conduct an impact assessment of the AI system develop a risk mitigation plan monitor the mitigation of the risks keep general records about the AI system publish the description of the AI system notify the users in case of "material harm" 	<p>AI and Data Commissioner and Ministerial powers</p> <ul style="list-style-type: none"> request information and records about the AI system, require audits, stop the operation of the AI system should they believe that there is a "serious risk of imminent harm" 	<p>Penalties; not meant to be punitive</p> <ul style="list-style-type: none"> fine of no more than \$10 million and 3% of the person's gross global revenues in the year <p>Offences attracting criminal liability</p> <ul style="list-style-type: none"> possession or use of data obtained through an offence under federal or provincial law <u>and</u> operation of an AI system knowing that it could likely cause physical or psychological harm or property damage could lead to a <ul style="list-style-type: none"> fine of no more than \$25 million and 5% of the gross global revenues in the financial year, as well as up to five years (minus a day) of imprisonment

"Artificial intelligence just blows my mind. I don't know where it's gonna go. I have a bigger fear of that than anything else in this world because if AI gets to the point with decision making on its own without any human intervention, it's a problem for mankind. And this is the piece that worries me. There needs to be...some good government legislation and control over AI."

Member of the General Public

Data & Innovation Recommendation 1

Data Stewardship Committee

RATIONALE

The current health privacy legal regime in Canada was developed when much of the health system was still paper-based. There is a need to ensure that health privacy laws can be responsive to a growing data and innovation landscape. There is an increasing call for legal reform and policies to specifically address the risk and potential harms from AI. “Artificial intelligence (AI) systems are poised to have a significant impact on the lives of Canadians and the operations of Canadian businesses.”⁶

RECOMMENDATION

- a) Include a section in PHIA that states that the Minister must appoint a Data Stewardship Committee (DSC) (akin to Alberta’s HIA ‘multi-disciplinary data stewardship committee).
- b) In the absence of a regulatory framework for AI in Canada, ensure that the DSC has the interim responsibility for establishing policies, as well as role to oversee and monitor large scale data initiatives, including those that involve high volumes of PHI, commercially-driven innovation projects and AI-specific implementations across health. The DSC will be responsible for i) receiving innovation and AI use cases that custodians or researchers in the province are intending to implement or develop, ii) review algorithmic impact assessments and establish transparency requirements, iii) comment on ethical and social implications for innovations and AI and iv) providing input regarding the integration of health and social services information as a part of patient records. (Look to AB HIA and BC eHealth Act for proposed language)
- c) Ensure that the makeup of the committee is representative of the data community and includes members of the public, Indigenous communities and other special interest groups, as needed.

Data & Innovation Recommendation 2

Substantially Similar Status of PHIA

RATIONALE

It is critical to note that PHIA will likely require additional amendments in the future to align to Bill C-27 and in order to maintain its substantially similar status. The recommendations put forward in this report take into account these anticipated future changes so as to reduce any duplication of effort and / or the need to undo changes in the future that could possibly contradict the future regulatory environment.

RECOMMENDATION

Ensure substantially similar status of PHIA is maintained.

Data & Innovation Recommendation 3

Definition for AI

RATIONALE

There is often misunderstanding about what constitutes AI or what is meant by an “automated decision”. The *Access to Information and Protection of Privacy Act* (ATIPPA) review proposed a definition of “automated decision system”, that has been considered by some to be “overbroad”.⁷

RECOMMENDATION

Align PHIA to the definition of AI in Bill C-27 - AIDA and have all AI initiatives reporting to the DSC in the interim until such a time that substantially similar status is established and a regulatory framework for AI is developed.

Monitoring & Oversight

Nationally and globally fines have or are expected to increase under privacy laws, particularly for malicious acts. Notably, there has been an increase in oversight and enforcement measures in Bill C-27. Bill C-27 would increase maximum penalties and give the ability for the commissioner to recommend administrative penalties. Within the province, ATIPPA and PHIA are not cohesive with respect to oversight provisions.

“I think people don't realize there's rights involved and what their rights are with anything, and health records are important.”

Member of the General Public

Monitoring & Oversight Recommendation 1 **Biometric and Genetic Databases**

RATIONALE

Biometric and genetic information is considered by many to be the most sensitive of personal health information and often comes with inherently more risk as it relates to privacy.⁸

RECOMMENDATION

Include a duty to report all existing and newly established biometric and genetic databases to OIPC in the Act.

Monitoring & Oversight Recommendation 2

Increase Fines & Penalties

RATIONALE

Fines and penalties for violations under privacy laws, including health privacy laws, across the country have been steadily increasing. These measures are intended to deter misuse of data, and further encourage overall compliance. While not a singly sufficient resolution for non-compliance, fines and penalties aim to enhance modern protections of privacy for Canadians.

RECOMMENDATION

Update section 88 (offenses and penalties) to increase fines and penalties to account for modern recourse, such as outlined in ON PHIPA s.72.

Monitoring & Oversight Recommendation 3

Hybrid Model for OIPC

RATIONALE

PHIA currently provides the OIPC with ombudsman oversight, rather than the hybrid role adopted by ATIPPA, 2015. Consequently, there is no mechanism within PHIA, whether through the courts or through powers vested by the Commissioner, to compel compliance with the Act by custodians, except in relation to access and correction requests. A hybrid model adopted by ATIPPA essentially combines the ombudsman and order-making powers, such that "the processes of the ombudsman model remain, except that in the end, a recommendation carries much more weight and consequence."⁹

RECOMMENDATION

Align role of the OIPC to ATIPPA (hybrid model) to provide effective oversight and remedial powers. An alternative would be to allow the Commissioner to bring any matter resulting in a recommendation under 72(2)(c) and (d) to the Trial Division to seek enforcement of the Commissioner's recommendations if the custodian fails to or refuses to follow the Commissioner's recommendations.

Consent

There is a significant need to modernize how we obtain consent for the collection, use and disclosure of PHI. Such modernization must include the ability for capable minors to consent to the collection, use, and disclosure of their own PHI. Additional considerations include de-identification standards and protection of the resultant data, as well as Indigenous consent.

“I think there is a bit of difference in values. I think for Inuit, written documents are often suspicious. So signing consent...it's not really informed consent. A lot of consent is based on relationships and trust. And sometimes that's not accepted within the healthcare system. I think there is a different value system that goes from the Indigenous perspective, very much based on the collective whereas the white government system is based on the individual rights.”

Indigenous Community Representative

Consent Recommendation 1

Capable Child

RATIONALE

Many custodians have struggled to provide consistent processes around PHI of minors, particularly regarding who has ultimate decision-making regarding access to and protection of privacy. According to the Newfoundland and Labrador Medical Association ("NLMA"), "PHIA does not establish an age at which someone can access their own record. The RHAs are using the age of 16 as this is the age of consent for treatment. This means a parent or guardian controls the access to the record and a youth cannot access their information without parental consent, nor can they restrict or deny the parent or guardian's access. The PHIA does not have a process by which a youth can request control over their own record."¹⁰

RECOMMENDATION

- a) Address the issue of mature minors in both the Act and the regulations by aligning the Act with ON and other jurisdictions, as deemed appropriate.
- b) Add to s.23 specifications regarding conflict if the child is capable that the child's wishes prevail as stated in ON's PHIPA.
- c) Build similar guidance as outlined below from ON to guide decision-making in the context of consent and sharing PHI of a capable child.

"A custodian may obtain consent for the collection, use and disclosure of personal health information from a capable child, regardless of age. As discussed above, individuals are capable of consent if they are able to understand information relevant to deciding whether to consent to the collection, use or disclosure of their personal health information, and to appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing their consent. If the child is less than 16 years old, a parent of the child or a children's aid society or other person who is lawfully entitled to give or refuse consent in the place of the parent may also give, withhold or withdraw consent. However, this does not apply in the context of information that relates to treatment within the meaning of the Health Care Consent Act, about which children have made a decision on their own, or counseling in which children have participated on their own under the Child and Family Services Act. A parent does not include a parent who has only a right of access to the child. If there is a conflict between a capable child who is less than 16 years old, and the person who is entitled to act as the child's substitute decision-maker, the decision of the capable child regarding giving, withholding or withdrawing consent prevails."¹¹

Sharing De-identified Data without Consent

RATIONALE

There are reported inconsistencies across the provinces regarding the interpretation of the meaning of 'anonymized' and/or de-identified data. As well, sharing of PHI that is believed to be either anonymized or de-identified is often undertaken without assurance that the PHI has identifiers sufficiently and irrevocably removed.

RECOMMENDATION

a) Update s.21 of the Act to include de-identification and add anonymization specifications to the regulations. This should provide rules regarding disclosure of information (without consent) if data is de-identified or anonymized, in alignment to Bill C-27. Also leverage the a) Information and Privacy Commissioner of Ontario, Health Information and Privacy - PHIPA Decision 175, March 25, 2022, PHIPA DECISION 175 (ipc.on.ca), b) Information and Privacy Commissioner of Ontario, June 2016, De Identification Guidelines for Structured Data.¹²

Supporting Indigenous Data Sovereignty

RATIONALE

The Committee heard that Indigenous communities have been seeking to have an Indigenous identifier added to patient records in the province for many years. It was expressed that an identifier would support data as belonging to an Indigenous person. This identifier could be leveraged by Indigenous communities to ensure that appropriate data flows for patient care and policy development. Overtime, the identifier has the potential to support Indigenous data sovereignty, as communities will be positioned to make or promote better decisions based on their own data.

RECOMMENDATION

- a) In consultation with Indigenous communities, implement a provincial Indigenous identifier(s) in order to support Indigenous data sovereignty and consent.
- b) Update s. 23 (consent provisions) of the Act to recognize specific elements of consent for Nunatsiavut government, as well as other Indigenous communities where appropriate, regarding the collection, use and disclosure of PHI. Specifically, consent may be provided orally and may involve community consultation and/or other considerations that reflect Indigenous cultures and values.
- c) Move the Nunatsiavut government out of the Regulations and list them as a custodian in s.4(1) of the Act.

Literacy & Social License

The public must be more aware of privacy legislation and their rights in order to make informed choices about their own PHI. Data literacy is needed for Canadians to understand and be aware of data messages that are meant to increase transparency.

There is a gap in Canadians' understanding of data and how it is used, which may hamper potential legislative changes. Transparency is a key pillar for privacy laws around the globe and is the backbone of a social license to leverage data for good.

“But the next piece is that I don't think that there's a lot of training that goes along with the current legislation. I think with any new legislation, that training component is essential.”

Member of the General Public

RATIONALE

There is increasing recognition of the need to engage patients and the public on matters relating to data sharing. In fact, the Pan-Canadian Health Data Strategy states, "The public and health workforce must be educated, active, and involved partners in the journey to improve data capability and capacity. In addition to education, there must be channels for diverse public voices to be expressed and embedded in the development of solutions. Establishing transparency as a key practice will be crucial to build and sustain trust."¹³

No formal mechanism or council exists today to establish a social license for NL's participation in pan-Canadian efforts and its own desire to share health data.

RECOMMENDATION

Establish a citizen's council. Include a mandate for education and awareness on access and privacy rights, data and digital literacy. Ensure the citizen's counsel provides input and acts as a resource to the DSC. The Government should engage the citizen's council on matters relating to the provision / inclusion of health and social services data and policies regarding health data sharing.

Literary & Social License Recommendation 2

Expanded Purpose to Support Beneficial Health Data Sharing

RATIONALE

Although provisions exist within PHIA to support data use and sharing (with and without consent) under particular circumstances, such as for health research that has been approved by the Health Research Ethics Board, there is often disagreement as to whether the Act supports responsible data use and sharing.

RECOMMENDATION

Include the following purpose in the Act: “to enable health information to be shared and accessed, where appropriate and where the benefits proportionally outweigh the risks of harm, (i) to provide health services, (ii) manage the health system, (iii) enable research, evaluation and innovation.”

Literary & Social License Recommendation 3

Maintaining a Register of Accesses & Disclosures

RATIONALE

Modern health privacy laws are founded on the principle of transparency. Despite this, it has not always been easy to access or view logs of accesses and disclosures. Demands for data are increasing provincially, nationally, and internationally and as such, it will be important for custodians to be able to produce lists of such authorizations.

RECOMMENDATION

To ensure that PHI is appropriately accessed and disclosed, add a requirement to the Act or Regulations that require custodians to maintain “a register that contains the identity of the natural or legal persons that have been granted access and to whom PHI has been disclosed, a description of the information accessed and/or disclosed, its origin, the purposes for which the access or disclosure was authorized, the duration of and conditions applicable to each authorization, including any security measures, and the processing time for the request for authorization”.

Other

There are recommendations that evolved throughout the consultations that the Committee believed to be important, but did not fall into one of the key theme categories. Nevertheless, the following recommendations are included for consideration.

Other Recommendation 1

Abandoned Records

RATIONALE

As custodians retire, there have been increasing numbers of abandoned records. When records of PHI are abandoned, it is difficult for patients to access their PHI. As well, there are problems ensuring accountability.

RECOMMENDATION

Align to ON to include a provision to allow the Commissioner to inquire or investigate abandoned records without consent.

Clear Authority for PHR

RATIONALE

The province is moving forward with the implementation of its PHR. It has been unclear whether PHIA currently provides authority to provide access to patient's PHI through the PHR and ultimately who is accountable in the event of a breach.

RECOMMENDATION

Define a legislative authority in PHIA for the entity responsible for the data held within the PHR. This entity must be authorized to provide access to patient PHI directly to patients. Such legislative authority should also indicate how the entity will interact with the custodians who are contributing data to the PHR, specifically:

- in the event of a breach involving multiple custodians.
- a request for data from multiple custodians.

PHIA must clarify that the entity holding the PHR data is accountable for the privacy and security of that data once a custodian has disclosed the data into the PHR. Custodians are responsible for the PHI they contribute to the PHR only prior to disclosure into the PHR, when such data is within their custody and control. Further specificity can be provided in the regulations.

Other Recommendation 3

Redress when PHI Shared Across-Jurisdictions

RATIONALE

The OIPC and other oversight bodies are increasingly required to consult and collaborate on complex cases that involve data sharing across jurisdictions, private and public sector partnerships, and with multiple parties. As this trend continues, it will be critical that individuals have assurance that they may seek redress when PHI is shared across jurisdictions.

RECOMMENDATION

a) Include ability for individuals to seek redress if their information has moved to another jurisdiction OR involves multiple parties and commercial activities (private sector) by adding to s.79 additional powers for the Commissioner for multi-jurisdictional data sharing, interoperability, AI and other complex data sharing breaches.

b) Add ability for the Commissioner to consult with and coordinate investigations with other jurisdictions.

2017 PHIA REVIEW (ROLLOVER RECOMMENDATIONS)

The below recommendations continue to be relevant for PHIA and are included in this report to ensure that the necessary amendments are implemented.

2017 no.	2017 PHIA Review Roll-over Recommendations
4	To better ensure legislative protection of personal health information by those practitioners regulated by the Health Professions Act, amend the Personal Health Information Act to designate all members of the professions listed in the Health Professions Act as “health care professionals” under Section 2(1)(j).
5	Amend the Act to make it clear that home support agencies are custodians.
12	To broaden the definition of “personal health information” to include information about any collection of body parts and bodily substance, amend the Act to replace the phrase “the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance” found in Section 5(1)(c) with the phrase “the collection, whether as part of a donation or not, of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance”.
22	In the interest of clarifying the difference between “research” and “evaluation”, and aligning with key frameworks, consider amending the Act to define “evaluation” to align with the definition developed by the Canadian Evaluation Society. Specifically, define “evaluation” as “the systematic assessment of the design, implementation or results of an initiative for the purposes of learning or decision-making”.
30b	Consider establishing regulations to the Act that require the oath or affirmation contemplated by Section 14(1) to be renewed at least once every three years.

CONCLUSION

This PHIA Review sought to find a balance between aligning PHIA to other health privacy statutes and trends across Canadian and even international privacy laws, while also considering what is unique to NL. Our culture, our people, geography and even differences to the type of PHI that is contained in records in this province is unique, particularly given the high prevalence of genetic diseases. Therefore, these features were relevant and considered throughout the Review.

As previously mentioned, the recommendations in this report aim to build a foundation for future changes that are expected with Bill C-27. The recommendations set out in this report will strengthen the foundation if and when these changes arrive.

Finally, the recommendations in this report are inspired from what we have heard in written submissions, survey responses and our consultations, particularly from patients, indigenous groups, and the general public. This report aims to offer a modern approach to access and privacy by taking courageous leaps in order to advance privacy and access for the people of this province.

REFERENCES

1. <https://www.infoway-inforoute.ca/en/component/edocman/6387-privacy-as-an-enabler-sharing-personal-health-information-for-interopability-primer/view-document?Itemid=103>
2. <https://www.ontariocanada.com/registry/showAttachment.do?postingId=37468&attachmentId=49462>
3. <https://www2.gov.bc.ca/gov/content/health/conducting-health-research-evaluation/data-access-health-data-central/data-management-oversight#:~:text=The%20DSC%20is%20established%20under,or%20a%20prescribed%20MoH%20database.>
4. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document>
5. <https://www.phiareviewnl.ca/documents/oipc-phia-review-submission-2023.PDF>
6. The Artificial Intelligence and Data Act (AIDA) – Companion document <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document>
7. <https://www.phiareviewnl.ca/documents/oipc-phia-review-submission-2023.PDF>
8. <https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/>
9. https://www.phiareviewnl.ca/documents/OIPC_PHIA_Review_Submission.pdf
10. <https://www.phiareviewnl.ca/documents/nlma-phia-review-submission.pdf>
11. <https://www.ipc.on.ca/wp-content/uploads/2015/11/hipa-faq.pdf>
12. <https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf>
13. <https://www.canada.ca/en/public-health/corporate/mandate/about-agency/external-advisory-bodies/list/pan-canadian-health-data-strategy-reports-summaries/expert-advisory-group-report-01-charting-path-toward-ambition.html>

APPENDIX A: CURRENT LEGISLATIVE LANDSCAPE - HEALTH PRIVACY LAWS OF CANADA

Alberta:

Personal Information Protection Act, Statutes of Alberta, 2003 Chapter P-6.5
Health Information Act, RSA 2000, H-5
Health Information Regulation, AR 70/2001.

British Columbia:

Bill 22-2021, See <https://www.leg.bc.ca/parliamentary-business/legislation-debates-proceedings/42nd-parliament/2nd-session/bills/progress-of-bills>.
BC Personal Information Protection Act, SBC 2003, CHAPTER 63

Federal

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5
("PIPEDA").

Manitoba

The Personal Health Information Act (C.C.S.M. c. P33.5)
Personal Health Information Regulation

New Brunswick

Personal Health Information Privacy and Access Act, S.N.B. 2009, c. P-7.05
General Regulation - Personal Health Information Privacy and Access Act

Newfoundland & Labrador

Personal Health Information Act, SNL 2008, c P-7.01
Personal Health Information Regulations, NLR 38/11

Northwest Territories

Health Information Act S.N.W.T. 2014, c.2
Health Information Regulations R-089-2015

Nova Scotia

Personal Health Information Act, SNS 2010, c 41
Personal Health Information Regulations, NS Reg 217/2012

Ontario

Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A
Ontario Regulation 329/04 General

PEI

Health Information Act, Chapter H-1.41
Health Information Regulations

Quebec

Protection of Personal Information in the Private Sector, chapter P-39.1.

Saskatchewan

Health Information Protection Act, H-0.021 ("HIPA")
The Health Information Protection Regulations, Chapter H-0.021 Reg 1

Yukon

Health Information Privacy and Management Act, SY 2013, c.16
Health Information General Regulation, YOIC 2016/159