Operational Review of the *Personal Health Information Protection and Access Act*

Department of Health

August 2015

New Nouveau Brunswick

Department of Health

Operational Review of the *Personal Health Information Privacy and Access Act*

Published by:

Department of Health
Government of New Brunswick
P. O. Box 5100
Fredericton, New Brunswick
E3B 5H1

Canada

Printed in New Brunswick

Print (Bilingual): ISBN 978-1-4605-0956-2
PDF (English): ISBN 978-1-4605-0957-9
PDF (French): ISBN 978-1-4605-0958-6

Table of Contents

Message from the Minister of Health

Since the time of antiquity, health professionals have guarded the privacy of their patients and New Brunswick's health-care providers readily accept this responsibility. However, as our 21st Century world becomes increasingly complex and information grows more accessible and portable, New Brunswickers need the legislative provisions provided by the *Personal Health Information Privacy and Access Act* (PHIPAA) to ensure their highly sensitive information is protected. However, this legislation must also be well understood by New Brunswick's health-care professionals and effective in its operation.

As part of the Act's provisions, PHIPAA had to be reviewed four years after coming into force to ensure that it was functioning as intended and shortfalls and challenges addressed. For the last year, the Department of Health has been consulting with stakeholders, especially health-information custodians, and the following report is based on their feedback. Almost universally, stakeholders felt that practical tools to educate health professionals about PHIPAA's application to their day-to-day work would be of great benefit to our province's health-care system. In addition, numerous changes to the Act were recommended to improve its functioning. An action plan to address the identified challenges has also been developed and is included in this document.

As Minister responsible for PHIPAA and its review, I wish to thank all of the participants of this process for their thoughtful submissions. The actions resulting from their feedback will benefit patient privacy and our health-care system.

Sincerely,

Hon. Victor Boudreau
Minister of Health

1.0 - Introduction

Information specific to an individual's health which could identify them is known as personal health information, regardless of the way that it is recorded or stored. It includes information that is oral, written or photographed.

Personal health information (PHI) is one of the most sensitive forms of personal information that exists. It can be about someone's mental or physical health, family history or health-care history. This includes genetic information, registration information, date of birth, information about payments or eligibility for health care or health-care coverage, information about organ or tissue donation, test results, or information that identifies a patient's health-care provider or substitute decision-maker.

In addition to being used for patient care, PHI is sometimes used for financial reimbursement, medical education, research, social services, quality assurance, risk management, public health regulation and surveillance, health planning and policy development.

This information is becoming increasingly accessible as technology evolves and becomes more portable at an exponential rate. As a result, jurisdictions across Canada have enacted legislation to protect the privacy, confidentiality and security of PHI.

In September 2010, the Government of New Brunswick enacted the *Personal Health Information Privacy and Access Act* (PHIPAA). PHIPAA provides a set of rules to protect the confidentiality, integrity and accessibility of PHI and the rights of the individual to whom the information relates.

PHIPAA does not apply unless the PHI is being collected or used to provide or assist in the provision of health-care services, the planning and management of the health-care system or for delivering a government program or service. The legislation specifically excludes PHI collected by employers (both public and private), insurance companies and regulatory bodies for health-care providers.

This Operational Review of the *Personal Health Information Privacy and Access Act* was conducted as per a requirement in Section 80 of the Act to examine how well it is functioning and what issues have been identified in its operation since its enactment in 2010. This final report is the result of an analysis of the feedback received from stakeholders throughout the review period and challenges that have been identified since the Act first came into force.

2.0 - Summary of the Review Process

The operational review of PHIPAA began in August 2014 with a comprehensive examination of the issues that the Department of Health compiled as they were identified since the Act came into force in September 2010. Generally, these items are matters that require clarification to make the administration of the Act more efficient or effective.

This information was then used in the development of a discussion paper that was released in January 2015 for public feedback and comment. The document pointed out a number of questions that have arisen over the years with respect to the definition of custodian; consent, both expressed and implied; and privacy impact assessments. Stakeholders and members of the public who wished to provide feedback on any matter pertaining to PHIPAA were asked to provide their input by the end of March 2015. Nine formal submissions were received through this process.

In addition, organizations that represent the bulk of New Brunswick's custodians of PHI were invited to participate in a one-day consultation session in February 2015 which included discussions about technology and privacy, custodial responsibilities, patient rights, and privacy breaches. Sixteen participants attended the session.

The chief privacy officers employed by the Department of Health, the regional health authorities, FacilicorpNB, the New Brunswick Health Council and Ambulance New Brunswick also participated in a section-by-section discussion of the Act and numerous meetings were held with Department of Health employees about how PHIPAA has impacted their work.

All of the feedback received has been compiled for use in the development of this final report.

3.0 - Stakeholder Input: What We Heard

3.1 - Strong Need for Greater Education

Throughout the operational review, it appeared that a culture shift is beginning inside New Brunswick's health-care system. Health professionals are increasingly cognizant of how their actions, even when they are well-intentioned, can impact patient privacy. This awareness has been brought about through deliberate efforts by custodians and the Office of the Access to Information and Privacy Commissioner to provide information to health professionals and the public about patient rights and custodial responsibilities under PHIPAA.

Education was seen by all stakeholders as a way to proactively prevent breaches, further sensitize health professionals to the implications of their actions and accelerate the culture change that is in progress.

Under PHIPAA, education and promotion of the Act is part of the mandate of the Access to Information and Privacy Commissioner. Custodians also have a duty to ensure their employees understand and work in accordance with the Act. However, while the consultation process made it clear health professionals understand they have responsibilities under the Act, the regulatory and professional organizations which represent them indicated that the education and training they are receiving from the custodians who are their employers is not meeting their day-to-day needs. This was also reflected in the comments received from the health professionals who participated in the review's consultation process. Almost universally, participants expressed concerns about the Act's complexity and their ability to appropriately interpret the legislation. They consistently expressed a desire for practical training on how PHIPAA applies to their day-to-day work so that they can use it to the benefit of their patients and their organizations.

This could potentially be achieved through partnerships between the Commissioner's office, professional associations/regulators and key custodians such as the regional health authorities and the Department of Health to develop appropriate learning materials for health-care professionals. Interactive training tools with real-world examples specific to the audience were identified as a potential solution.

In addition, the regulatory bodies who participated in the day-long consultation session for custodians expressed that the best way to prevent breaches is by ensuring that post-secondary education programs for health-care professionals include PHIPAA in their curricula so that new professionals will graduate with an awareness of their responsibilities under the Act. In addition, they recommended that their associations be informed of the general circumstances of a breach by a member so that they can help change behavior among those health professionals who are already practicing.

3.2 – Enhancing PHIPAA

3.2.1 - Incorporating the 10 Privacy Principles in Legislation

New Brunswick is one of three provinces whose health information protection legislation has been recognized as substantially similar to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). The other provinces are Ontario and Newfoundland.

It is advantageous for New Brunswick's personal health information protection legislation to be deemed substantially similar as "organizations that are subject to provincial legislation deemed substantially similar are exempt from PIPEDA with respect to the collection, use or disclosure of personal information occurring within the respective province."[1]

For a privacy law to be deemed substantially similar to PIPEDA, the legislation must: "provide privacy protection that is consistent with and equivalent to that found under PIPEDA; incorporate the ten principles in Schedule 1 of PIPEDA; provide for an independent and effective oversight and redress mechanism with powers to investigate; and restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate." [2] The 10 privacy principles found in Schedule 1 of PIPEDA are known as the "fair information principles" that are the basis of the Canadian Standards Association's *Model Code for the Protection of Personal Information*.

While PHIPAA was drafted with the 10 principles in mind, they were not specifically codified in the legislation as is the case with PIPEDA. As a result, custodians without knowledge of the privacy principles sometimes lack the benefit of the appropriate context when interpreting the legislation. During the consultation process, some custodians indicated that they were able to resolve many of the questions they received by explaining the 10 privacy principles and felt their inclusion in the Act would be of benefit to custodians and the public.

1 Canada. Office of the Privacy Commissioner of Canada. *Privacy Legislations in Canada*. Web. 22 June 2015.
2 Ibid

The 10 Privacy Principles

Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Limiting collection: The collection of personal information shall be limited to that which is necessary for the purpose identified by the organization.

Limiting Use, Disclosure and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Accuracy: Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Individual access: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Challenging compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

3.2.2 - The Definition of Custodian: Custody and Control

PHIPAA sets out the responsibilities of those who collect, maintain or use the PHI of New Brunswickers for a health-care purpose. These individuals are called custodians.

PHIPAA defines a custodian as "an individual or organization that collects, maintains or uses personal health information for the purpose of providing or assisting in the provision of health care or treatment or the planning and managing of the health care system or delivering a government program or service…"[3] The legislation then goes on to list a variety of individuals or organizations that are considered custodians. This includes public bodies, health professionals, the Minister of Health, health partner organizations such as the regional health authorities and Ambulance New Brunswick, information managers, health-care facilities such as hospitals and clinics, research data centres, researchers and nursing homes.

The definition of "custodian" has been the subject of many questions over the last four years. In practice, people and organizations who are designated as custodians under PHIPAA often work together to deliver a program or service. In these cases, it can be difficult to determine who is ultimately the custodian of the PHI being handled. PHIPAA does not recognize this scenario in its provisions which leaves a question as to how custodians are intended to respond to these situations.

The structure of the Act has also lead to a "Russian doll" problem where one custodian is functioning within a larger structure that is also deemed a custodian under the Act. For example, health-care facilities are designated as custodians under PHIPAA. However, hospitals and community health centres fall under the responsibility of a regional health authority, which is also considered to be a custodian. As all public health-care facilities in New Brunswick are part of one of the province's two regional health authorities, the question has arisen as to whether the dual designation is necessary.

Two of the submissions received suggested the definition of custodian should incorporate the notions of custody and control so as to clarify the roles and responsibilities of all those who manage patients' PHI. Ontario's *Personal Health Information Protection Act* was cited as an example of a jurisdiction which incorporates this concept by defining "health information custodian" as "a person or organization… who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties…"[4]

3.2.3 - Information Managers

Information managers hold a dual designation under PHIPAA. This has been questioned as to its necessity.

An information manager is a custodian who processes, stores, retrieves, archives, disposes and de-identifies, or otherwise transforms PHI on behalf of another custodian. Information managers are, for example, information technology firms or document disposal companies. Information managers in New Brunswick have the same responsibilities as other custodians under PHIPAA and are also required to a sign formal, written agreement with the custodian for whom they are providing the service explaining how they will secure and protect the PHI that they hold in accordance with the Act.

---

3 Personal Health Information Privacy and Access Act. *Acts and Regulations of New Brunswick*, P-7.05. New Brunswick. *Office of the Attorney General*. 2014. Web. 21. Oct. 2014.

4 *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sched. A. Ontario. *E-Laws*. 2015. Web. 6. July. 2015.

In personal health information privacy legislation in other Canadian jurisdictions, information managers are not custodians. Instead, they are recognized as a person or organization working on behalf of a custodian who is obligated to protect the PHI it manages according to the terms of its contract with the custodian who is responsible for the integrity and protection of the data.

The Department received three submissions on this topic. Two argued that information managers should not be custodians under the Act, given that their role is to support a custodian's business and they do not collect, use or disclose PHI for their purposes. One of these two submissions said it is superfluous to expect an information manager to enter into a written agreement to abide by a custodian's obligations under PHIPAA if they are already deemed to be a custodian. The third submission expressed support for maintaining wording.

3.2.4 - Special Custodians: Monitoring Agencies and Researchers

In New Brunswick, two organizations are responsible for the independent analysis of statistical information to assist in the management, evaluation and monitoring of the allocation of the province's health-care resources, health-system planning and the delivery of health-care services. These two organizations are the Canadian Institute for Health Information (CIHI) and the New Brunswick Health Council (NBHC).

CIHI data assists the Department of Health in monitoring system performance on a national scale and the NBHC is primarily responsible for measuring the quality of services being provided to New Brunswickers at a provincial level.

While the NBHC also collects PHI directly from New Brunswickers as part of its work, both organizations are secondary collectors of PHI, which is used in their reporting. This secondary data does not usually include names and addresses, but would include Medicare numbers. In the event that this PHI were inadvertently disclosed, it would be highly difficult for either organization to directly inform the affected individuals. Extracting information from their systems in order to provide patients with a copy of their PHI upon request would also be a complex process. As a result, both organizations are seeking special recognition in PHIPAA of their roles in the health-care system that would allow each of them to carry out their functions under a single data-sharing agreement (one per organization) with the Department and eliminate their responsibility to provide patients with access to information. This special status would not apply in cases in which the NBHC is the primary collector of PHI.

Questions have also arisen as to whether independent researchers should have the same rights to disclose PHI as other custodians. While it makes sense that researchers should be required to meet all of the Act's obligations with respect to the protection of PHI and be able to use the PHI they receive for their research purposes if appropriate security precautions are in place, it has been argued that they should not have the same rights of disclosure.

This challenge can be addressed in part through continued work to supply prepared and/or de-identified personal-level administrative data sets to the New Brunswick Institute for Research, Data and Training (NB-IRDT), which makes these data available to government, academic and other researchers on a restricted basis in a controlled, secure environment. In its submission, the NB-IRDT pointed out that research plays an important role in public policy development and proposed changes to PHIPAA and other legislation to remove unnecessary barriers to access to administrative data sets.

3.2.5 - Mandatory Disclosure of Personal Health Information

The Canadian Medical Protective Association (CMPA) expressed an objection to the sections of the Act that mandate a custodian to disclose personal health information without the consent of the individual in prescribed circumstances. In particular, the stakeholder expressed concerns that custodians are required to disclose personal health information, including information relating to a person providing health care to a person carrying out an inspection, investigation or a similar procedure authorized pursuant to Subsection 41(1) of PHIPAA. The association was particularly concerned that this disclosure could be made to police without a warrant, subpoena or court order and argued that this requirement could damage the trusting relationship between physicians and their patients.

The CMPA was also concerned that Paragraph 40(1)(a) and Subsection 41(1) require that the personal health information of a health-care provider be disclosed to police and regulatory authorities without regard to the relevance of that information and said that this mandatory disclosure requirement could potentially result in health-care providers failing to seek treatment.

The association argued that such disclosures should be permissive, not mandatory, and only made in clearly defined circumstances and that the relevance of the information to the investigation must be part of the considerations prior to any disclosure taking place.

3.2.6 - WorkSafeNB

WorkSafeNB was an active participant in the consultation session held for custodians and provided a detailed submission to the Department with respect to the challenges PHIPAA has presented to the ways that it collects, uses and discloses PHI in the normal course of its operations. It has asked that PHIPAA be reviewed to clarify privacy and consent issues that give consideration to its unique funding structure and the employer's role in the workers' compensation system.

Paragraph 38(1)(a) of PHIPAA allows custodians to disclose PHI without the consent of the individual for the purpose of determining or verifying the eligibility of that individual to receive services or benefits provided under an Act of the legislature. However, the Act requires those services or benefits be funded, in whole or in part, by the Province or the Government of Canada. This clearly excludes the disclosure of PHI by custodians to WorksafeNB, which is entirely employer funded. However, it seems unlikely that the protection against fraud this section affords government-funded programs was not intended to apply to government-mandated programs as well. Amending this section of the Act would validate WorkSafeNB's responsibility to communicate with health-care providers and provide information to employers that is necessary for the purpose of administering the *Workers' Compensation Act*.

3.2.7 - Substitute Decision-makers

In the event that an individual is unable to consent to the collection, use or disclosure of PHI, Subsection 25(1) of PHIPAA outlines who may do so on the individual's behalf. During the consultation, stakeholders provided feedback that Paragraphs 25(1)(d), (e) and (f) should be reviewed in consideration of the complexities of a 21st Century family life. Paragraph 25(1)(d) indicates that an individual's spouse or common-law partner may fulfill the role of substitute decision-maker, but this clause does not take into consideration situations in which a couple may be separated and involved in another relationship, but not divorced, which has periodically posed an issue for the regional health authorities. Paragraph 25(1)(e) indicates that an individual's adult child can play

the role of substitute decision-maker, but does notcontemplate multiple adult children with differing opinions. Paragraph 25(1)(f) gives a non-custodial parent the same decision-making rights as the custodial parent.

3.2.8 - Administration of the Act

As stated previously, the Department of Health has been collecting a list of questions or issues that have arisen since the Act came into force in September 2010. This list was then used in the development of the discussion paper that was released as part of the PHIPAA review.

There are several matters that have been identified over the years that should be examined. Generally, these matters are points of clarification or differences of interpretation between the French and English versions of the Act that would make its administration more effective and efficient. Amendments to the Act may be required as a result.

For example, paragraph 37(5)(b) of the Act states that a custodian **may** disclose PHI relating to an individual who is deceased "for the purposes of informing a person whom it is **reasonable** to inform in the circumstances of the fact that the individual is deceased or presumed to be deceased and the circumstances of the death, **if appropriate.**" (Emphasis added.) Custodians indicated this paragraph sometimes poses challenges for health professionals as it contains so much subjectivity.

Section 9 of the Act sets out how a custodian may accommodate an individual's request for access to their PHI if the record is not available in the individual's official language of choice. Custodians have different interpretations of their obligations under the Act depending on whether they use the French or English versions of the Act. Furthermore, the Official Languages Commissioner has pointed out that individuals who receive their medical file in a language other than the one of their choice are not aware of their right to assistance and believes that custodians should be obligated to inform patients of their right.

Other examples include a request to provide custodians such as dentists and pharmacists with clear authority to electronically disclose PHI to life and health insurers for payment purposes. Canadian Blood Services is seeking greater clarity that the donation of blood, stem cells or organs are included in the definition of health-care under PHIPAA so that the PHI collected from donors is clearly protected by the Act.

3.2.9 - Including Auditing Provisions in Legislation

PHIPAA includes provisions requiring custodians to protect PHI by adopting information practices that include reasonable administrative, technical and physical safeguards that ensure the confidentiality, accuracy and integrity of the information. These practices must be based on nationally or jurisdictionally recognized information technology security standards and processes, appropriate to the PHI to be protected. In so doing, they are expected to implement controls to ensure that the PHI collected is being used as authorized under PHIPAA and confirm that agents of the custodian adhere to the safeguards that have been put in place.

Auditing employee access to electronic health records is considered to be a recognized and effective way to confirm that no inappropriate access to PHI has occurred. Custodians who were consulted as part of the PHIPAA review indicated that while auditing does occur when they are investigating a suspected breach, random/routine audits happen less frequently and are therefore not a deterrent to individuals who are looking at files without a legitimate purpose. Some stakeholders suggested that adding auditing requirements to PHIPAA would help to address this issue.

3.3 - Privacy Impact Assessments and Data-sharing Amongst Health Partners

As noted previously, PHIPAA requires that reasonable administrative, technical and physical safeguards be undertaken that ensure the confidentiality, accuracy and integrity of the information. Routine audits, are used to determine whether PHI has been collected, used or disclosed in accordance with the Act. The conduct of privacy impact assessments and the development of data-sharing agreements occur before any collection, use or disclosure of PHI to prevent breaches and ensure PHI is being managed with PHIPAA and the 10 privacy principles in mind.

3.3.1 - Privacy Impact Assessments

A privacy impact assessment evaluates the information governance practices of a specific program, to determine if they respect legislative requirements and where a privacy risk might exist.

Subsection 56(1) of PHIPAA requires that public bodies or any other custodian prescribed by regulation conduct privacy impact assessments for the new collection, use or disclosure of PHI or any change to the collection, use or disclosure of PHI.

However, properly conducting such an assessment can involve a significant investment in staff time and, if a consultant is contracted to provide support for the activity, has financial implications as well. As a result, New Brunswick's health-care organizations are seeking greater precision in the legislation as to when a privacy impact assessment should be conducted.

Federal government policy respecting privacy impact assessments is more defined.

Specifically, a privacy impact assessment is generally required when a federal government department:

- Uses or intends to use personal information in a decision-making process that directly affects an individual;
- Substantially modifies existing programs or activities where personal information is being used, or intended to be used, in a decision-making process that directly affects an individual;
- Contracts out or transfers a program or service to another level of government or the private sector resulting in substantial modifications to a program or activity;
- Substantially redesigns the system that delivers a program to the public, or;
- Collects personal information which will not be used in a decision-making process that directly affects an individual but which will have an impact on privacy.[5]

3.3.2 - Data-sharing Agreements

A data-sharing agreement is a formal contract that clearly documents what data are being shared and how the data can be used. Such an agreement serves two purposes. First, it protects the custodian providing the data, ensuring that the data will not be misused. Second, it documents the context and conditions under which sharing would occur.

The Department of Health, the regional health authorities and the New Brunswick Health Council routinely share data to determine or verify the eligibility of an individual to receive health-care services, determine

5 Canada. Office of the Privacy Commissioner of Canada. *Fact Sheet: Privacy Impact Assessments*. Web. 23 June 2015.

or provide payment for the provision of a health-care service, or to deliver, evaluate or monitor a health-care program. This data flows over information technology networks maintained by the Department of Government Services and FacilicorpNB.

This information should flow in accordance with data-sharing agreements, and agreements have been developed for new collections, uses or disclosures of PHI since PHIPAA came into force. However, not all transactions presently follow data-sharing agreements and it would be impossible to document every instance of data sharing that occurs between these health organizations. As a result, it was recommended that consideration be given to an umbrella data-sharing agreement that governs their activities or a legislative provision that would recognize their special status as custodians who must share data for the proper operation of the province's health-care system.

3.4 - Inconsistencies with Other Acts

During the review process, the Department of Health was advised of three Acts which contain sections that are not consistent with PHIPAA.

3.4.1 - *Mental Health Act*

Subsection 4(3) of PHIPAA states that the provisions of *Mental Health Act* prevail over PHIPAA. Section 17 of the *Mental Health Act* outlines the confidentiality provisions specific to mental health information. The Act generally prohibits the disclosure of any information relating to the mental condition, observation, examination, assessment, care or treatment of the person while a patient of a designated psychiatric facility.

Subsection 17(4) of the *Mental Health Act* states that an administrator of a psychiatric facility may disclose information for the purposes of research, academic pursuits or the compilation of statistical data. Under subsection 17(7), the researcher is not permitted to disclose the name or any means of identifying the patient or former patient.

The administrator of an individual hospital should not be expected to process a request from a researcher for information. These requests would be more properly managed by the regional health authority at a corporate level as the custodian responsible for the custody and control of the data. The *Mental Health Act* also lacks provisions that can be found in PHIPAA that stakeholders feel should apply to mental health information such as data matching, consent, and general safeguard requirements.

3.4.2 - *Right to Information and Protection of Privacy Act*

Subsections 6(1) and 6(2) of PHIPAA state that the *Right to Information and Protection of Privacy Act* (RTIPPA) does not apply to PHI in the custody or under the control of a custodian unless PHIPAA specifies otherwise. Custodians to whom RTIPAA applies have interpreted these subsections to mean that it is not possible to receive PHI unless an individual is applying for access to his or her own data or unless specifically authorized under PHIPAA.

This opinion is further supported by Subsections 21(1) and 21(2) of RTIPPA which deem the disclosure of PHI to a third party to be an unreasonable invasion of an individual's privacy.

It is, however, possible for a third party to use RTIPPA to request record-level data that has been de-identified in accordance with PHIPAA and is therefore no longer PHI. Under PHIPAA, the term 'de-identified', means PHI from

which all identifying information has been removed. The release of this data under RTIPPA would make it part of the public record without any restrictions placed upon the applicant as to its use, protection or destruction.

The use of RTIPPA to gain access to large amounts of de-identified PHI poses three concerns for the custodians to whom RTIPPA applies:

- In a province with a small population base equivalent to a medium-sized Canadian city spread through many small communities, custodians questioned whether it was possible to truly de-identify record-level data. In the case of an individual with a rare condition or disease, that person's gender and the name of their community might be sufficient to identify them.
- If a large quantity of records is requested, custodians expressed a lack of confidence in their ability to guarantee they could remove all identifying elements as per their obligation under PHIPAA.
- Under PHIPAA, researchers are required to meet stringent standards, including having their project vetted by a research ethics board and signing a data-sharing agreement, before PHI is shared with them. Processing a request for such a large amount of data under RTIPPA rather than PHIPAA could open backdoor for individuals who did not want to follow appropriate channels for their work.

There can be no debate that the public has a right to public records held by a public body. However, custodians are recommending amendments to PHIPAA and/or RTIPPA to ensure broad requests for record-level PHI by third parties under RTIPPA are treated as research requests and therefore subject to appropriate safeguards.

3.4.3 - *Archives Act*

PHIPAA does not apply to the *Archives Act*, but the two Acts are not consistent with the respect to when PHI would become a releasable part of the public record.

Paragraph 3(2)(b) of PHIPAA states that the Act does not apply to an individual's PHI if (i) 100 years have passed since the record containing the information was created, or (ii) 50 years have passed since the death of the individual. Once PHIPAA ceases to apply to a record in the possession of the Department of Health or the regional health authorities, it can no longer be protected from disclosure.

However, Department of Health and regional health authority files are sent for storage at the Provincial Archives well before 100 years after the creation of the record.

While paragraph 10(3)(b) of the *Archives Act* recognizes the need to protect personal information (PHI is a form of personal information) by ensuring that public records are not available for public inspection if doing so would reveal personal information concerning another person; paragraph 10(4)(a) of the Act states that the Provincial Archivist may make these records available for public inspection 100 years following the date of birth of the person to whom the personal information relates.

When the *Archives Act* was created in 1977, the average life expectancy of a Canadian citizen was 70 years for men and 77 years for women.[6] By 2011, average life expectancy had increased to 79 years for men and 83 years for women.[7] It is no longer unusual for an individual, particularly a woman, to live into her early 90s. This means that a record being held by the Provincial Archives containing PHI could potentially be made available for public inspection only a few years after a person's death or, in a few cases, while they are still alive.

6 Canada. Statistics Canada. *Life expectancy increased steadily throughout the 20th Century*. Web. 2 July 2015.
7 Ibid.

4.0 Three-Year Action Plan

The Department of Health will undertake the following actions to address the varying issues that have been identified by custodians and other stakeholders as part of the Operational Review of the Personal Health Information Privacy and Access Act.

Year 1

Greater Education

- Establish a working group of key stakeholders to:
  - » Develop practical educational tools for front-line health-care professionals;
  - » Meet with post-secondary schools to better understand how PHIPAA is incorporated into their educational programs for health professionals;
  - » Discuss how regulators of New Brunswick's health professionals can actively participate in building an improved understanding of PHIPAA amongst their members and work with custodians when breaches occur.

Enhancing PHIPAA

- Explore amendments to PHIPAA to bring greater clarity to its provisions respecting access to PHI in one's language of choice; address operational issues identified by WorkSafeNB; and ensure that the donation of blood, tissue or organs is recognized as health-care under the Act.
- Develop and finalize an agreement with FacilicorpNB as an information manager for New Brunswick's health-care system.
- Ensure any unnecessary barriers to research using administrative data sets are removed.

Privacy Impact Assessments and Data-Sharing Amongst Health Partners

- Initiate discussions with respect to an umbrella data-sharing agreement between the Department of Health, the regional health authorities, the New Brunswick Health Council and Ambulance New Brunswick.

Years 2 and 3

Enhancing PHIPAA

- Explore potential amendments to PHIPAA to provide greater clarity for custodians when interpreting Act; remove the requirement that information managers also be custodians and incorporate the concept of custody and control into the definition of custodian; recognize the role that monitoring agencies such as CIHI and the NBHC play in the monitoring and evaluation of the effectiveness and efficiency of NB's health system; clarify provisions with respect to substitute decision-makers and privacy impact assessments; include the 10 privacy principles in the Act; ensure that the individual's right to privacy in their PHI supersedes the public's right to information; and address inconsistencies with other Acts.
- Consult with the regional health authorities about reasonable auditing provisions and establish these provisions in legislation.

- Conduct a jurisdictional review of the disclosure provisions in similar legislation across Canada and consult with regulatory bodies to determine best practices with respect to disclosure of personal health information without the consent of the individual in prescribed circumstances.
- Ensure that the provisions of the *Mental Health Act* with respect to the disclosure for research purposes are considered in a modern context in any potential review of the *Mental Health Act*.

Privacy Impact Assessments and Data-Sharing Amongst Health Partners

- Continue work on an umbrella data-sharing agreement between the Department of Health, the regional health authorities, the New Brunswick Health Council and Ambulance New Brunswick.

5.0 Acknowledgements

The Department of Health wishes to officially acknowledge the numerous people who contributed their time, knowledge and experience to this Operational Review.

Access to Information and Privacy Commissioner Anne Bertrand and her staff provided the Department with detailed feedback on the content of the discussion paper prior to its release and conducted a presentation during the consultation session that was held with associations and organizations which represent the province's custodians of PHI.

The Chief Privacy Officers of the Department of Health, the regional health authorities, FacilicorpNB, the New Brunswick Health Council and Ambulance New Brunswick were extremely generous with their time and participated in a line-by-line review of PHIPAA and the operational challenges it has presented. Their guidance and feedback was invaluable.

The Department received written submissions from the following individuals and organizations:

- The Canadian Medical Protective Association;
- Canadian Life and Health Insurance Association;
- Office of the Commissioner of Official Languages for New Brunswick;
- FacilicorpNB;
- Comité des 12;
- Canadian Institute for Health Information;
- WorkSafeNB; and
- Dierdre L. Wade, Q.C.
- New Brunswick Institute for Research, Data and Training.

The following associations and organizations representing New Brunswick custodians of PHI participated in the day-long consultation session:

- Réseau de santé Vitalité;
- Horizon Health Network;
- WorkSafeNB;
- Department of Government Services;
- Velante;
- New Brunswick Association of Social Workers;
- New Brunswick Medical Society;
- New Brunswick Nurses Association;
- New Brunswick Dental Society;
- New Brunswick College of Pharmacists; and
- New Brunswick Chiropractors' Association.