PHIA Amendment Review

Winnipeg Regional Health Authority Recommendations Report for Amendments to The Personal Health Information Act

The Personal Health Information Act of Manitoba, enacted in 1997, was the first standalone health information protection law in Canada. It has set the tone for how Personal Health Information is managed through provincial legislation. Built into the Act is a mandatory five year cyclical review. This Report provides amendment suggestions from the perspective of the Winnipeg Regional Health Authority, the largest health services provider in Manitoba, and comments on where PHIA has remained effective in the twenty years since its enactment, where it has begun to show signs of age, as well as areas in which it is currently silent but that need to be addressed.

June 23, 2017

For information contact:

Christina Von Schindler
Chief Privacy Officer
Winnipeg Regional Health Authority
4th Floor, 650 Main Street
Tel: 204-926-7049
cvonschindler@wrha.mb.ca

Transmittal Letter

June 23, 2017

PHIA Review
Legislative Unit
Manitoba Health, Seniors and Active Living
Main Floor, 300 Carlton Street
Winnipeg, MB
R3B 3M9

Re: Review of *The Personal Health Information Act*

I am pleased to enclose the Report of the Winnipeg Regional Health Authority in response to the invitation of the Ministers of Health, Seniors and Active Living and of Sport, Culture and Heritage to participate in the public consultation process being conducted as part of the review of *The Personal Health Information Act*.

The size and scope of the WRHA makes it uniquely positioned to provide insight into how PHIA has remained effective in the twenty years since its enactment, where it has begun to show signs of age, as well as areas where it is currently silent but which need to be addressed.

The WRHA wishes to express its appreciation for the opportunity to participate in and to contribute to the review, and looks forward to further consultations as improvements and additions to PHIA are identified and discussed.

Yours truly,

Allister Gunson
General Counsel and Corporate Secretary

AG/ak
Encl.

Table of Contents

Introduction

The Personal Health Information Act (PHIA), enacted in 1997, was the first standalone health information protection law in Canada. It has set the tone for how Personal Health Information (PHI) is managed through provincial legislation. Built into PHIA is a cyclical review. Accordingly the Ministers of Health, Seniors and Active Living and of Sport, Culture and Heritage announced a public consultation process on changes to PHIA and to its companion legislation *The Freedom of Information and Protection of Privacy Act* (FIPPA). This Report has been prepared in response to the invitation to provide input on PHIA, and contributes amendment suggestions from the perspective of the Winnipeg Regional Health Authority, the largest health services provider in Manitoba and the trustee of vast quantities of the health information of Manitobans, in both paper and electronic formats.

The WRHA serves the Winnipeg-Churchill Health Region which consists of the City of Winnipeg, the rural municipalities of East and West St. Paul, and the northern community of Churchill, representing a total population of more than 700,000 people. The WRHA also provides health care support and specialty referral services to nearly half a million Manitobans who live outside the Region, as well as to residents of northwestern Ontario and Nunavut, who often require the services and expertise available within the WRHA.

Among the largest employers in Manitoba, the WRHA employs more than 27,000 people. With an annual operating budget of $2.5 billion, the WRHA is the largest health authority in the province, and in addition to its own operations, operates or funds over 200 health service facilities and programs. The size and scope of the WRHA makes it uniquely positioned to provide insight into how PHIA has remained effective in the twenty years since its enactment, where it has begun to show signs of age, as well as areas where it is currently silent but which need to be addressed.

The recommendations in this Report are informed by:

1) The lived experiences of the WRHA and Manitoba eHealth in the collection, use and disclosure of PHI within the rubric of existing legislation,

2) A cross-jurisdictional analysis of legislation in other Canadian provinces and territories for indicators of how others may have managed common considerations, and

3) A comprehensive stakeholder engagement process and survey to capture the perspective of WRHA leadership, staff, program areas, partners, patients and families with regards to how PHIA informs their daily lives and interactions with the WRHA as well as what they see as opportunities for strengthening the provisions of PHIA.

PHIA concerns itself with two overarching considerations: the rights of individuals and the obligations of trustees. PHIA underscores that PHI belongs to the individual that the information is about and sets out the rights of individuals to privacy of their PHI, to view and receive copies of their own PHI, as well as to request correction to their PHI maintained by a trustee where it is inaccurate or incomplete.

PHIA recognizes that trustees need to collect PHI in the delivery of health care services as well as to make use of that information for related purposes as provided for in PHIA. The second primary focus of PHIA is therefore establishing the roles and obligations of trustees with regard to the PHI that they are entrusted with in the delivery and planning of health care.

PHIA has remained largely effective in accomplishing its purpose of protecting individual privacy. This is an observation supported by the stakeholder engagement survey conducted by the WRHA leading up to the drafting of this Report in which 97.78% of the 900+ respondents responded that PHIA protects privacy landing in the "perfectly well to somewhat well" response range. Only 2.22% of respondents thought that PHIA does not protect the privacy of Manitobans well.

Where PHIA has shown signs of age is in keeping up with the evolution of how health care is delivered and organized in Manitoba. The stakeholder engagement survey found that where respondents most saw room for improvement were in the areas of better understanding of electronic management and communication of PHI, as well as when PHI may reasonably be shared especially in a partnership service delivery model where stakeholders may not all be trustees or delivering a health service as defined in PHIA.

Indeed a great deal has changed in how health care is organized and delivered in the twenty years since PHIA came into effect. Drafted largely from the perspective of standalone health practitioners in a paper-based charting system and in anticipation of a more electronic health information landscape, there are notable gaps in addressing roles, responsibilities and accountabilities for PHI in which health services are largely delivered through multi-disciplinary partnerships and organized through electronic or hybrid health record systems to which there are multiple trustee contributors. It is also silent on disclosure of the PHI of Manitobans beyond Manitoba territorial borders as is addressed in the legislation of some other jurisdictions. In an environment where, increasingly, requests are made for Pan-Canadian analysis as well as where information management options are increasingly cloud-based, this is an area that merits consideration.

In addition to the aforementioned rights and responsibilities, PHIA is organized around three primary activities of a trustee in dealing with PHI: the collection, use and disclosure of PHI, and outlines what is permissible in these activities and related considerations under each. This

Report is organized accordingly with suggested content for inclusion in PHIA as pertaining to the primary activities and obligations of a trustee.

The goals of the recommendations of this Report can be summarized as follows:

- Ensuring that PHIA remains current and responsive within a rapidly changing and increasingly digitized environment.
- Reducing barriers to appropriate and timely access to health information by both individuals and health professionals.
- Improving capacity for clear and effective communication between health services professionals towards timely and efficient care provision in a multi-disciplinary environment of care delivery partnerships.
- Clarifying and formalizing appropriate secondary purposes of PHI while ensuring transparency, accountability and privacy protection.
- Increasing transparency, accountability and support for valued research while ensuring privacy and the confidentiality of PHI.
- Formalizing transparency and accountability of trustees, their employees and agents, and towards ensuring breach prevention, whether inadvertent or wilful.

Interestingly, after twenty years PHIA still presents some challenges. There is not yet a consensus on the breadth and depth of trustee obligations in protecting PHI. While intended to be an enabling piece of legislation that does not interfere with the delivery of health care, it is pointed to at times as an impediment to health care delivery. Many still believe that a piece of PHI can have only one trustee at a time, and do not recognize that in an electronic world a piece of information can be viewed simultaneously by multiple people so that there can be numerous trustees of the same item of PHI. The full implications of the use in PHIA of the term "trustee" have not been fully appreciated. At law, "trustee" is a well-defined term which invokes the full body of trust law and of fiduciary obligations. One would assume that the term, being so well known in law, was chosen intentionally so as to invoke those fiduciary obligations (and anecdotal conversations with people involved in the creation of PHIA confirms this), but in practice that has not occurred. We do not yet have an understanding of what are the rights under PHIA of minors and of their parents, and of deceased individuals. There is still uncertainty on how security safeguards are required for a medical practitioner with 2000 paper charts as opposed to a service provider with 4 billion bytes of electronic data, and how each is to audit those safeguards. Police services are trustees under PHIA when they come into possession of PHI – do they know that and what obligations they incur as a result? Should there be specific rules for how police officers use and disclose PHI?

Ultimately, the goal of this Report and the recommendations for amendments to PHIA is to strike a workable balance between protection of privacy and the authority and accountability of

trustees and their agents that rely on access to PHI in order to deliver, plan and research health care services in Manitoba.

In conjunction with their invitation for public input into the review of PHIA, the Ministers issued a discussion document entitled "*A Review of The Personal Health Information Act: Tell Us What You Think*". This discussion document posed a number of questions. A list of the questions, with responses, is attached as Appendix 1 to this Report. It also informed a number of the comments throughout this Report.

The WRHA welcomes this review of PHIA and is appreciative of the opportunity to provide input into the public consultation on its improvement. PHIA is a piece of legislation that operates at two levels: as an enactment that sets out principles and policies, and as a living document that guides the conduct of health care providers and organizations in their daily activities. It is because of the direct impact of PHIA on those activities and on how health care is delivered, and is delivered effectively, that the WRHA also requests that it be actively involved in the ongoing consultation process and eventual deliberation of changes to be made to PHIA as part of this cyclical review.

1. Defined Terms

As is often the case with legislation, the definitions section is the underpinning of PHIA, as the terms used and their definitions reflect the concepts upon which PHIA operates. The following are some specific changes and additions proposed to the definitions section of PHIA; there are also changes that are referred to later in the body of this Report in connection with specific issues.

1.1 *Roles of Trustees and Agents*

While PHIA is about protecting the PHI of individuals, most of its provisions address the roles, obligations and responsibilities of trustees. Sometimes PHIA is erroneously viewed as "enabling" trustees to deal with PHI – in fact, for the most part, PHIA is the opposite: it places obligations on trustees which are designed to protect the PHI of individuals. And it is that goal of protecting PHI that raises questions whether the current definition of trustee is cast sufficiently broadly.

PHIA requires trustees to ensure that employees receive training and have appropriate limitations imposed upon their activity involving PHI. It further underscores that employees may not act in any manner that the trustee would not be authorized to do so under PHIA. In 2010, PHIA was amended by creating specific offences for individuals, including the provision of an offence by "an employee, officer or agent" of a trustee under Subsection 63(2). Though this inclusion enabled the objective of holding employees accountable for willful breaches of PHIA, and thereby buttressed the ability of employers also to do so, there remains opportunity for strengthening the provisions of PHIA to address not only increased individual accountability but also for greater clarity of roles, authorities and accountabilities. For example, many of those individuals are either employees of the trustee (e.g., most nurses, most allied health care professionals, health care aides, and administration and support staff), or engaged by the trustee as independent contractors (most physicians), and are already trustees in their own right under PHIA. Therefore their obligations to comply with PHIA may exist both directly and under the terms of their employment or engagement contract.

In addition, there are individuals who have access to PHI, may be involved in the collection and recording of PHI, and so on, who act in capacities other than as employee or engaged contractor and who are not already trustees. For example, most health care facilities are reliant on the services and dedicated work of volunteers, who provide direct support and assistance to patients and to their families. Education and training are vital activities in the health care system, as students in the various health care fields are given practical "hands-on" training and exposure to patients and to the delivery of health care. Liability insurance is a vital tool in

allowing most trustees (individuals and organizations) to function in what can be a fairly litigious environment. It is a requirement of liability policies that the insured give notice to the insurer of possible claims (usually defined as facts that may indicate a possibility that a claim may be made against the insured). The reporting of possible claims occurs all the time, yet it may not fall fully within Paragraph 22(2)(k) of PHIA.

How should adequate protection be provided for the PHI that may have been disclosed to volunteers, students and participants in the liability insurance process? PHIA does not adequately address this, and Subsection 63(2) of PHIA applies only to employees, officers, and agents of a trustee. "Agent" already has a well-defined meaning in the law; and it may not include these additional groups. One solution might be to include them in the definition of "trustee". However that has undesirable implications. A more desirable approach is to define "agent" as including the foregoing persons. Whichever method is chosen, it will also be necessary to enable such use and disclosure (which often occurs out of necessity today) in the other provisions of PHIA, notably Sections 21 and 22.

An example of a relevant definition found in the legislation of another jurisdiction is the Yukon's *Health Information Privacy and Management Act*, which provides:

> 2(1) "agent" of a custodian means a person (other than a person who is prescribed not to be an agent of the custodian) who acts for or on behalf of the custodian in respect of personal health information, including for greater certainty such a person who is
> (a) an employee of the custodian,
> (b) a person who performs a service for the custodian under a contract or agency relationship with the custodian,
> (c) an appointee, volunteer or student,
> (d) an insurer or liability protection provider,
> (e) an information manager,
> (f) if the custodian is a corporation, an officer or director of the corporation, or
> (g) a prescribed person;

With some changes, this might be suitable for our PHIA.

The opportunity should also be taken to confirm exactly what is meant by use of the term "trustee". "Trustee" invokes the extensive body of law on trusts, and imposes fiduciary obligations (sometimes described as the strongest obligations under the law). Is it intended that a PHIA trustee holds PHI in trust? Is it intended that the extensive obligations and restrictions on trustees in regards to the trust property they hold apply equally to PHI? Or is PHIA, in conjunction with FIPPA and *The Privacy Act*, meant to be an exhaustive code of how PHI is to

be protected in Manitoba? For example, some jurisdictions use the term "custodian" as opposed to "trustee". If it is intended that "trustee" be read in PHIA in its full legal sense, it would be helpful to clarify this by inserting some confirming language. If it is not, then perhaps a different term (such as "custodian") may be appropriate.

1.2 *Personal Health Information & De-identified Information*

PHIA defines PHI as recorded information about an identifiable individual that relates to the individual's health or health care history. It does not govern activity involving PHI that has been de-identified, as such information no longer constitutes PHI as defined. There is a significant divergence of understanding however about what may reasonably be considered as de-identified individual level health information and when protections under PHIA may or may not still be applicable. PHI which has been de-identified or anonymized may in fact not be sufficiently de-identified so as to prevent the identification of the individual in question, or to prevent it readily being "re-identified" (i.e., used in conjunction with other available information) to identify the individual.

The terms "identifiable", "de-identified" or the closely related "potentially identifiable" are not defined in Manitoba law. Individual trustees have developed their own policy definitions and standards with regards to these considerations. However, there is at present no Manitoba-wide standard for what protections may be afforded to the privacy of individuals by imposing limitations on the collection, use, and disclosure of individual level health information that has been stripped of unique direct identifiers but whereby potentially identifiable individual level information remains.

The absence of legislated definitions and protections for potentially identifiable health information has meant that limits to the secondary collection, use and disclosure of this information have been open to inconsistent interpretation by trustees and their agents of whether certain data is PHI and subject to the protection of PHIA. This creates a situation of disagreement and misunderstanding between trustees and their affiliates regarding risk and protection requirements for individual level information that may have direct identifiers removed but sufficient quasi-identifiers remaining to place the information at risk of being re-identified.

One could even question whether such concerns are appropriate under PHIA as currently worded. The WRHA believes that they are, but guidance in PHIA is desirable.

Risks associated with potentially identifiable health information were significantly less prevalent in the paper-based environment of 1997. In today's increasingly digitized data environment,

however, where big data is becoming common-place and available to any PC end-user, the considerations of what may constitute "de-identified" and "identifiable" bear revisiting.

A commonly cited example of the potential re-identifiability of de-identified data can be found in the work of Latanya Sweeny[1], current Director of the Privacy Data Lab at Harvard University, who as a Masters Student in 1996 using only publically available information correctly re-identified 87% of a cohort of a "de-identified" dataset containing only individual zip code, age, gender and date of birth.

In the years since Sweeney's groundbreaking work, access and volume of publically available personal information has grown exponentially as has the risk for malicious or inadvertent re-identifiability of "de-identified" data not expressly subject to protections under PHIA. This awareness places responsibility on trustees to take additional measures beyond that required by law to impose limits on all individual level data whether bearing unique identifiers or some combination of quasi-identifiers that may, by themselves or in combination with other available data, breach individual privacy. The absence of an overarching legislated provision for this highly interpretative activity places risk not only on individual privacy but also undue burden of accountability on trustees, end-users, and researchers, who may not be experts in data management and analysis, to determine what may be considered potentially identifiable.

Therefore it is desirable that PHIA recognize that there is a category of data which is not at the moment PHI but which is readily capable of being re-identified to become PHI, and that as a result that data must be protected. However, the possibility of re-identification must be more than theoretical – otherwise trustees will never know if the former PHI is now sufficiently de-identified to fall outside of PHIA. And the circumstances of re-identification change with knowledge and technology. Therefore it is recommended that PHIA address this issue. The options would appear to be:

- include in the definition of PHI de-identified data which meets a certain standard of "re-identifiability", or
- confirm that de-identified data is clearly excluded from PHIA.

We consider the first approach to be the desirable one. Therefore, we suggest that PHIA be amended to include a provision such as:

[1] Sweeney, Latanya *Simple Demographics Often Identify People, Carnegie Mellon University,* Data Privacy Working Paper 3, Pittsburgh 2000, p. 2.

> **"re-identifiable health information"**[2] means information that was once but is no longer personal health information as a result of the removal of the details that allow for the identification of the individual to whom such personal health information related, and which:
>
> (i) does not identify the individual,
>
> (ii) in circumstances reasonably foreseeable to the trustee is not capable of being utilized, either alone or with other reasonably available information, to identify the individual; and
>
> (iii) is not prescribed in the Regulation as such;

and that the definition of PHI be amended to include re-identifiable heath information.

There still remains the possibility of uncertainty whether information which is de-identified and which is not "re-identifiable health information" is not covered by PHIA. This could be addressed by a suitable wording change to Section 3 of PHIA so as to confirm that such information is outside the scope of the legislation.

In redefining PHI to mean information at the individual level that retains sufficient levels of quasi-identifiers, a provision may be added to clearly delineate that information that is partially or wholly de-identified and compiled solely for secondary purposes of the trustee as authorized in PHIA is not subject to an access request. This may be accomplished under Part II of PHIA as a reason for refusal as suggested in a following section of this Report.

An alternate approach to ensure protection of potentially identifiable health information may be to define that term and to impose separate considerations and limitations than for directly identifiable PHI. This approach, though better than current circumstances, is not recommended as the preferred course of action as it leads to greater risk to privacy than providing protections to all individual level health information.

Some examples are:

> **"potentially identifiable health Information"**[3] is information that has had all identifiers removed that identify the individual, but that retains some number of quasi-identifiers that may, in combination with other available data, serve to re-identify the individual the information is about.

[2] Definition adapted from the Nova Scotia, *Personal Health Information Act.*
[3] Definition adapted from the Nova Scotia, *Personal Health Information Act.*

> **"quasi-identifier"** refers to an element of information in reference to an individual that when combined with other quasi-identifiers may serve to re-identify a previously de-identified health data.

Potentially identifiable health information must be matched to other known or available data in order to be re-identified. It is further recommended that consideration be given to making it an offence under PHIA to willfully match the potentially identifiable PHI to any other data except as permitted by PHIA or by a written agreement with the trustee.

These recommendations would serve to further limit opportunities and inadvertent risks through the misunderstanding that PHIA protections apply to directly identifiable (bearing names) information only. They would further serve to facilitate effective and transparent use of PHI for secondary purposes by eliminating mixed interpretations between parties and related standards for disclosure and related protection measures such as requirements for agreement, records of user activity, etc.

1.3 *Data Matching*

Closely related to the considerations of re-identifiability is the issue of data linkages or "data-matching", or the joining of one or more sources of available data for a unique individual. As discussed above, a key consideration of what may reasonably be considered as de-identified is whether the person holding the data set may reasonably be expected to have access to other sources of information that, if matched, may serve to re-identify an individual and result in a breach to their privacy.

Currently PHIA does not define nor contemplate activity involving multiple data sets beyond the authority of the Manitoba Ombudsman to comment as provided for in Paragraph 28(e)(i).

> 28 In addition to the Ombudsman's powers and duties under Part 5 respecting complaints, the Ombudsman may
> (e) comment on the implications for the confidentiality of personal health information of (i) using or disclosing personal health information for record linkage

There are provisions surrounding data matching in the legislation of other Canadian jurisdictions including Alberta and New Brunswick. The Office of the Saskatchewan Information and Privacy Commissioner has issued a discussion paper on Data Matching.[4] In addition to instructing on

[4] https://oipc.sk.ca/assets/data-matching.pdf

the issues and controls that should be considered, such legislation and the discussion paper highlight the importance of defining the scope of any legislative provisions. Therefore it is recommended that, in addition to recognizing the privacy risk inherent in individual level data, PHIA take the additional measure to define "data matching" as well as provide limitations and commensurate authorities and protections for this activity.

An example of such protections is inherent in the change in definition for PHI that would include an addition to provisions for the secondary use and disclosure of individual level PHI, as proposed above and later in this Report, that require that any health information about a unique individual used or disclosed for a secondary purpose be de-identified to the greatest extent possible while meeting the requirements of the authorized purpose, and that there be assurance of commensurate protections against subsequent unauthorized use, disclosure, and matching of the data.

The following definition and provisions are recommended for consideration:

> **"data matching"**[5] means the creation of identifying or potentially identifying information by combining information from two or more electronic data bases or two or more electronic records or otherwise available data.
>
> No person may use or disclose personal health information for data matching except as authorized in this section.
>
> A trustee shall not
> (a) collect personal health information for the purpose of being used in data matching except as authorized in this Act;
>
> A trustee may perform data matching using personal health information in its custody and control, provided that the collection, use or disclosure of the personal health information being used for data matching or created as a result of data matching is authorized in this Act.
>
> A trustee may use or disclose personal health information for data matching for a secondary purpose provided that personal health information is first de-identified to the greatest extent possible and the use and disclosure of the resulting personal health information is authorized by sections 21 and 22.
>
> If data matching is performed for research purposes, the conditions of section 24 must be met.

[5] Data and provisions adapted from New Brunswick, *Personal Health Information Privacy and Access Act.*

1.4 *Use and Disclosure*

The activities of "use" and "disclose" are fundamental to PHIA. (The term "disclose" appears 30 times, and the term "use" appears 39 times.) Interestingly, these terms are not defined. While their normal meanings are likely intended, some further guidance would be helpful. The following examples may be considered:

> **"disclose"**[6] in relation to information, includes releasing information or making information available in any manner or format, including verbally or visually, to a person;
>
> **"use"**[7] includes accessing, handling, dealing or reproducing information, but does not include disclosing the information.

[6] Definition adapted from the North West Territories *Health Information Act.*
[7] Definition adapted from the New Brunswick *Personal Health Information Privacy and Access Act.*

2. Primary and Secondary Purposes

PHIA recognizes that a trustee may need to collect, use and disclose PHI for the purpose of providing health care. PHIA also recognizes that there are other lawful purposes for which a trustee may need to use or disclose the PHI within its custody and control. The distinction between the provision of health services and of other lawful purposes is commonly referred to in the literature as a distinction between primary and secondary purposes.

In 2001, the Government of Canada created Canada Health Infoway to accelerate the adoption of digital health information solutions in Canada[8]. The years since have seen a dramatic rise in the accumulation of vast stores of digital health data that may be looked to for a variety of valuable purposes that are in the public best interest, such as disease mapping.

2.1 *Definitions*

Government departments and Regional Health Authorities (RHAs) may have further need to use PHI for the planning, delivery and evaluations of health services. These considerations are touched upon in Subsection 21(a) of PHIA which provides that:

> 21 A trustee may use personal health information only for the purpose for which it was collected or received, and shall not use it for any other purpose, unless
> (a) the other purpose is directly related to the purpose for which the personal health information was collected or received;

as well as Subsections 21(d) and (e):

> (d) the trustee is a public body or a health care facility and the personal health information is used
> (i) to deliver, monitor or evaluate a program that relates to the provision of health care or payment for health care by the trustee, or
> (ii) for research and planning that relates to the provision of health care or payment for health care by the trustee;
> (e) the purpose is one for which the information may be disclosed to the trustee under section 22;

[8] Canada Health Infoway website: https://www.infoway-inforoute.ca/en/about-us , accessed January 2017.

Similarly, Paragraph 22(2)(a) of PHIA concerns itself with disclosure to someone who is or will be providing or has provided health care to the individual, to the extent necessary to provide health care to the individual (a primary purpose), and the balance of Subsection 22(2) sets out a list of other considerations (secondary purposes), some of which are discussed in greater detail later in this Report.

The terms "primary purpose" and "secondary purpose" are commonly used in the discussion of PHI and personal information and have been adopted in the laws of some other jurisdictions. It is recommended that Manitoba also formally define what may be considered a primary purpose of a trustee as well as to more clearly articulate what may be meant by other lawful or secondary purposes. Some suggestions include:

> **"primary purpose"**[9] means the purpose for which personal health information was originally collected, and includes any purpose that is consistent with that purpose;
>
> **"secondary purpose"** means any use or disclosure of PHI for a purpose beyond the primary purpose for collection.

Secondary purpose includes Data Matching, Planning and Management, Evaluation, Surveillance and Research for the purposes of PHIA.

2.2 *Research v. "research"*

The term research is used in two different contexts and meanings in PHIA: in Section 21 what is in effect "administrative research" and which is a use by a trustee, and in Section 24 which is true research and which is a disclosure by a trustee. So as to remove sources of misunderstanding, it would be helpful to clearly distinguish between the two different uses of the term.

Currently Paragraph 21(d)(ii) states that:

> A trustee may use personal health information only for the purpose for which it was collected or received, and shall not use it for any other purpose, unless
> (d) the trustee is a public body or a health care facility and the personal health information is used
> (ii) for research and planning that relates to the provision of health care or payment for health care by the trustee;

[9] Definition sourced from Saskatchewan *Health Information Protection Act.*

For the purpose of clarity, it is recommended that Paragraph 22(d)(ii) be amended by replacing the term "research and planning" with "planning and management", as defined below, to reduce misunderstanding and the misapplication of this provision of PHIA to research activity governed under Section 24.

> **"planning and management"**[10] includes
> (a) the collection, analysis or compilation of information with respect to
> (i) the administration, management, evaluation or monitoring of the health system, including for Quality Improvement
> (ii) the allocation of resources to the health system, or
> (iii) planning for the health system, and
> (b) public health surveillance;

Accordingly, the following definitions are also recommended:

> **"quality improvement"** includes, in respect of the health care or other related programs or services that a trustee provides
> (a) risk management activities,
> (b) error management activities,
> (c) activities to enhance patient safety, and
> (d) any other activities that maintain or improve the programs or services;

> **"public health surveillance"**[11] means the ongoing, systematic collection, analysis and interpretation of health data for the purposes of monitoring, describing, planning, evaluation and implementation of public health and public health services, interventions and programs.

It bears mention that there are additional secondary purposes, most notably for education of health care professionals, that are clearly recognized by other jurisdictions that will be discussed in greater detail below.

[10] Definitions for planning and management and quality improvement adapted from the Yukon's *Health Information Privacy and Management Act.*
[11] Definition adapted from that employed by the US Centre for Disease Control.

3. Access to PHI

PHIA provides for the right of individuals to access their own PHI maintained by trustees. Section 5 establishes their right upon request to examine and receive a copy of one's PHI. Subsection 6(1) imposes an obligation on trustees to respond to such requests "promptly" and within assigned time limits:

> 6(1) A trustee shall respond to a request as promptly as required in the circumstances but not later than
> (a) 24 hours after receiving it, if the trustee is a hospital and the information is about health care currently being provided to an in-patient;
> (b) 72 hours after receiving it, if the information is about health care the trustee is currently providing to a person who is not a hospital in-patient; and
> (c) 30 days after receiving it in any other case, unless the request is transferred to another trustee under section 8.

A trustee must render assistance to a requestor:

> 6(2) A trustee shall make every reasonable effort to assist an individual making a request and to respond without delay, openly, accurately and completely.

and take steps to protect confidentiality while responding:

> 9 A trustee
> (a) shall not permit personal health information to be examined or copied without being satisfied as to the identity of the individual making the request; and
> (c) shall take reasonable steps to ensure that any personal health information intended for an individual is received only by that individual.

The above provisions are applicable to all trustees, from sole practitioners, to hospitals, to RHAs. When a patient is personally known to an independent health services provider, locating a record and establishing identity, and following up with the applicant directly, if needed, are routine considerations. However, when a trustee is a hospital and/or a RHA, where personal familiarity is less likely, and which receives multiple requests that are handled by a Health Information Services department for processing, certain challenges at times arise with the trustee's capacity to complete an access request within the time frames set out in PHIA.

Somewhat unique to the WRHA is that it is the trustee of:

- the PHI of the patients in its hospitals or who received health care through its community and long-term care programs, and
- the PHI contained in the various electronic health information systems that it maintains, many of which are provincial in scope.

3.1 *Abandoned Requests*

As a large health care organization, the WRHA frequently receives access requests with insufficient information to process the request. PHIA provides that a trustee may require a request to be in writing and the WRHA has produced a form with fields for all necessary information in order to respond to a request. However, there are circumstances where requests are received verbally, by telephone, or by fax that, absent additional information and/or follow-up with the individual, cannot be processed as received.

These situations commonly include:

- Where there is insufficient information provided in a request for access to be able to locate or to uniquely identify the record being requested. For example, the WRHA periodically receives requests for historical records from individuals or their representatives without sufficient information for the WRHA to be able to process the request.
- Where the trustee has determined that fees are applicable and has informed the individual, but the individual does not respond with payment nor with a request for a waiver of fees, and efforts to contact the individual further have been unsuccessful.
- Where the copies of the requested PHI have been made and have been waiting for a period of time to be picked up at the individual's request, and attempts to contact the individual to establish another method of delivery have proven unsuccessful.

In such circumstances, the trustee is still under an obligation in PHIA to respond within the prescribed time frame. And there are occasions where documents in response to a request have been prepared and at the direction of the requestor are being held for pickup from the trustee, and the pickup never occurs. In such situations, technically the trustee must maintain that response on hand indefinitely.

Subsection 82(3) of FIPPA deems a request to have been abandoned if the requestor does not respond to a fee estimate within 30 days.

> 82(3) The applicant has up to 30 days from the day the estimate is given to indicate if it is accepted or to modify the request in order to change the amount of the fees, after which the application is considered abandoned.

Similarly, Alberta's *Health Information Act* Subsection 9(1) has included provisions for when a request for access may be considered abandoned, as follows:

> 9(1) Where a custodian contacts an applicant in writing respecting the applicant's request, including
> (a) seeking further information from the applicant that is necessary to process the request, or
> (b) requesting the applicant to pay a fee or to agree to pay a fee,
> and the applicant fails to respond to the custodian, as requested by the custodian, within 30 days after being contacted, the custodian may, by notice in writing to the applicant, declare the request abandoned.

It is recommended that PHIA include a provision that clearly outlines when a request for access may reasonably be considered abandoned. This would include when a trustee has responded to an application request in a manner required by PHIA for:

(a) seeking additional information from the applicant required to complete the request,
(b) informing the applicant of applicable fees to process the request, or
(c) when an applicant has not picked up or been available to receive the requested records, and no further response has been received from the applicant,

and after a set period of time (e.g., 30 days) has passed with no further action by or communication from the requestor.

3.2 *Authority to Disregard Certain Requests*

FIPPA authorizes public bodies to disregard certain requests as follows:

> 13(1) The head of a public body may disregard a request for access if he or she is of the opinion that
> (a) the request is incomprehensible, frivolous or vexatious;
> (b) because of their repetitious or systematic nature, the requests would unreasonably interfere with the operations of the public body or amount to an abuse of the right to make those requests; or
> (c) the request is for information already provided to the applicant.

Currently there is no equivalent provision in PHIA, though to the extent that a trustee is a public body and holds personal information, FIPPA Subsection 13(1) applies to it.

Nova Scotia's *Personal Health Information Act* provides that:

> 64(1) Where a custodian believes on reasonable grounds that a request for a record of user activity is
> (a) frivolous or vexatious; or
> (b) part of a pattern of conduct that amounts to an abuse of the right of a request for a record of user activity, the custodian may refuse to grant the request.
> (2) When a refusal is made under subsection (1), the custodian shall provide the individual with written notice that sets out the reasons for the refusal and states that the individual is entitled to make a complaint to the Review Officer about the refusal.

and

> 81(1) Where a custodian believes on reasonable grounds that a request for access
> (a) is frivolous or vexatious; or
> (b) is part of a pattern of conduct that amounts to an abuse of the right of access,
> the custodian may refuse to grant the request.
> (2) When a refusal is made under subsection 72(1) or subsection (1), the custodian shall provide the individual with written notice that sets out the reasons for the refusal and that states that the individual is entitled to make a complaint about the refusal to the Review Officer.
>
> 89 Where a custodian believes on reasonable grounds that a request for a correction
> (a) is frivolous or vexatious; or
> (b) is part of a pattern of conduct that amounts to an abuse of the right of correction,
> the custodian may refuse to grant the request and shall provide written notice to the individual.

It is recommended that Manitoba include a similar provision in PHIA, such as:

> 11(3) Where a trustee, after having met the trustee's duty to assist under subsection 6(2) of this Act, reasonably believes that a request for access, a record of user activity, or a correction is
> (a) incomprehensible, frivolous or vexatious;
> (b) part of a pattern of conduct that amounts to an abuse of the right of a request under this Act; or
> (c) because of their repetitious or systematic nature, the requests would unreasonably interfere with the operations of the trustee or amount to an abuse of the right to make those requests;
> the trustee may refuse to grant the request.

11(4) In the circumstances mentioned in subsection (3), the trustee shall, where demographic information is known, respond in writing and state in the response given under section 11(3)
(a) that the request is refused and the reason why;
(b) the reasons for the trustee's decision; and
(c) that the applicant may make a complaint to the Manitoba Ombudsman about the refusal.

4. Restrictions on Use

Section 21 of PHIA specifies that PHI may be used by a trustee with consent of the individual, for the purpose that it was collected, or without consent for another purpose provided that "other purpose is directly related to the purpose for which the personal health information was collected or received".

4.1 *Education Purpose*

Education and training are integral parts of the health care delivery system. Students, interns, residents, and others who are training in the health care field are active observers and participants in the provision of health care.

PHIA does not explicitly recognize education as an authorized secondary use of PHI. As quoted above, it does permit secondary use for purposes closely related to the reason for collection. Trustees who use PHI for the purposes of educating their workforce must rely on an interpretation of Section 21 that the education of care providers is a purpose closely related to the primary purpose for collection or the provision of care. However, given that education is an important consideration in its own right, and is already inextricably tied up with the delivery of health care, education should be expressly authorized by PHIA. In so doing, PHIA could formalize current practices and provide trustees the stated authority to use or disclose PHI for the purposes of a legally defined "education purpose" provided that, in accordance with Subsection 20(2), the activity be limited to only those persons that need to have it for an authorized purpose and to the minimum amount necessary for that purpose.

For example, Alberta's *Health Information Act* provides:

> 27(1) A custodian may use individually identifying health information in its custody or under its control for the following purposes:
> (e) providing for health services provider education;

It is therefore recommended that Sections 21 and 22 of PHIA be amended to include "education purpose" as an authorized reason for secondary use and disclosure of PHI. A suggested definition is as follows:

> **"education purpose"** means an activity involving the use or disclosure of personal health information for the purpose of instruction that is conducted outside of the direct provision of care and as part of a formal learning or training program conducted by the trustee or associated with a formal learning program of an educational institution and authorized by the trustee.

4.2 *Information Purpose*

The list of permitted uses of demographic information in Section 21 does not include notification of events or opportunities that the trustee reasonably believes may be in the interest of that individual. A recently cited example involved wanting to send invitations to a specialized summer camp for children with a specific health circumstance. Another commonly cited purpose is informing patients and/or families of the formation of a patient group that they may have an interest in taking part.

The WRHA recommends that consideration be given to amending Section 21 of PHIA to include provision for the secondary use of demographic information for the purposes of informing an individual of a matter or service that the trustee reasonably believes would be acceptable to the individual. But in doing so, recognition is given to two important caveats:

- The use of demographic information for this purpose be conducted in a manner that reasonably ensures that it does not reveal specific information about the health of the individual to anyone not authorized to have this information; and
- Protections be put into place to protect patients from the marketing of goods and services in which the trustee or others have a financial profit-based interest.

How to draw the distinction between the benign and well-intentioned on one part and promotion for financial self-interest is difficult, and further deliberation will need to be given to how such a distinction can be made so as to offer valuable opportunities to address their health needs but protect them from being targeted for what they would consider to be unacceptable purposes.

5. Restrictions on Disclosure - Masking

Paragraph 22(2)(a) of PHIA provides:

> 22(2) A trustee may disclose personal health information without the consent of the individual the information is about if the disclosure is
> (a) to a person who is or will be providing or has provided health care to the individual, to the extent necessary to provide health care to the individual, unless the individual has instructed the trustee not to make the disclosure;

There are multiple challenges with complying with the stated exception of "the individual has instructed the trustee not to make the disclosure". It would appear that the exception assumes that the PHI is maintained in a single paper record or file. There is usually only one such paper record or file, and the instruction not to disclose can easily be noted on it. Plus Paragraph 22(2)(a) deals with disclosure "to a person". While this could be read as including a general prohibition on disclosure, if a specific person is named then the identity of that person must clearly be set out. Electronic information systems do not lend themselves to either of these activities.

While an electronic record may be maintained by one trustee, often multiple trustees will have access to it. Authorizations to access are usually granted to the system and not to specific files on the system. So, unless the instruction is given that no one may access the file of a specific patient (which begs the question why the file is there), it is not feasible with such systems to block the access of specified individuals to access the file of a specific patient. For example, if Ms. Jones instructs that her lab results are not to be disclosed to Dr. Smith, once those lab results are placed in a synoptic electronic record system such as eChart Manitoba, it is not possible to block electronically the access by just Dr. Smith to those specific lab results or to Ms. Jones' entire file. To complicate matters, the ability to mask the identity of a patient, or to block access to a patient's file, varies greatly between systems.

Having said that, it is recognized that there are very legitimate reasons for protecting patient data from being seen by others, such as the contact particulars of an abused spouse.

The electronic patient record (EPR) system used in many Winnipeg hospitals allows for the designation of who may access the file of a specific patient, but then renders the patient invisible on the system to anyone who has not been so designated. Because of the tremendous effort in tracking and maintaining such designations, and most importantly the likely adverse impact to patients when a health care provider who was not previously designated (for example, an Emergency Department physician) cannot locate the patient in the EPR, this functionality is

not used. Further thought needs to be given to this part of Paragraph 22(2)(a), and how allowing patients to protect their PHI from access by certain named persons can be accommodated with electronic health information systems. As currently worded, the provision cannot be complied with fully.

eChart Manitoba has attempted to address this issue by use of "disclosure directives". These directives are posted on the patient's electronic file in eChart, so that anyone who attempts to access the patient's file must undertake additional steps acknowledging that there is a disclosure directive. To proceed to see the record is known as "breaking the glass", and all such events are then subject to follow-up by Manitoba eHealth and the person accessing the file must justify having done so. There is a concern that the presence of a disclosure directive, and the consequent accountabilities of the person who breaks the glass, may deter some health care providers from breaking the glass so that the health care provided to the patient may be adversely affected.

While the foregoing discussion has focussed on whether disclosure may be made of PHI, it is not clear whether an instruction given pursuant to Paragraph 22(2)(a) prevents the use of that PHI by a trustee. Section 21 of PHIA sets out a number of situations where use is permitted, and Section 22 is only one of them.

6. Electronic Data Systems and Refusing Access

Electronic health information systems are intended and designed to allow for multiple persons to contribute information and to access information. This can provide some challenges.

PHIA Subsection 11(1) sets out specific and limited circumstances in which an individual's request for access to PHI may be refused. Paragraphs 11(1)(a), (b) and (c) provide:

> 11(1) A trustee is not required to permit an individual to examine or copy his or her personal health information under this Part if
> (a) knowledge of the information could reasonably be expected to endanger the health or safety of the individual or another person;
> (b) disclosure of the information would reveal personal health information about another person who has not consented to the disclosure;
> (c) disclosure of the information could reasonably be expected to identify a third party, other than another trustee, who supplied the information in confidence under circumstances in which confidentiality was reasonably expected;

Because there is often a disconnect between the person who enters the PHI into the system (and hence may have an appreciation of the factors set out in those Paragraphs) and the person who maintains the systems and receives the access requests (and who likely has no familiarity with the factors set out in those Paragraphs), the ability to fulfill Subsection 11(1) is greatly constrained. It is recognized that the language of the Subsection is permissive and not directive. If there is any expectation that the trustee will proactively address those Paragraphs and ensure that the intended protections will always be applied, there is no assurance that this will be the case.

Similarly, under *The Protecting Children (Information Sharing) Act* (PCIS Act), which is expected to be proclaimed into effect soon, Subsection 3(1) allows for the disclosure of information by a trustee, and Subsection 3(2) then provides:

> 3(2) A service provider or trustee may make a disclosure under subsection (1) only if they reasonably believe that the disclosure is in the child's best interests.

The trustee who is in the best position to make the assessment whether disclosure is in the child's best interests is usually the trustee who collected it and caused it to be entered into the information system. The trustee who receives the request under the PCIS Act is likely a different person, or a different operation within the trustee, who is not necessarily in a position to make the required assessment under Subsection 3(2).

7. Record of User Activity

A Record of User Activity (RUA) is a requirement under the *Personal Health Information Regulation* (Regulation) and is defined in Section 1 as:

> "**record of user activity"** means a record about access to personal health information maintained on an electronic information system, which identifies the following:
> (a) individuals whose personal health information has been accessed,
> (b) persons who accessed personal health information,
> (c) when personal health information was accessed,
> (d) the electronic information system or component of the system in which personal health information was accessed,
> (e) whether personal health information that has been accessed is subsequently disclosed under section 22 of the Act;

In addition to the Regulation, there are ministerial guidelines (Guidelines for Records of User Activity (RUA)) that provide further instruction to trustees related to RUAs.

7.1 *Subsequent Disclosures*

Subsection (e) of the RUA definition ("subsequently disclosed") cannot be accommodated by electronic health information systems. A paper record likely has a limited number of users, and as PHI in that record is accessed and then subsequently disclosed, this can be recorded if necessary in the paper file. With an electronic health information system, the trustee who maintains the system has no way of determining whether PHI accessed was subsequently disclosed by another trustee who accessed it from the system. So the onus is on the trustee who accessed and then subsequently disclosed the PHI to keep such a record and then to enter that information into the RUA. Most, if not all, of the WRHA's current electronic systems do not have provision for entering notations of this nature. And it is highly unlikely that health care providers working in a busy environment such as a hospital ward or clinic will have the opportunity to stop and to record each time a subsequent disclosure of the PHI was made. At some point they will likely have forgotten which system the PHI was ultimately accessed from. Compound this with the hundreds of trustees who may access systems such as eChart Manitoba in a day. Subsection (e) is not realistic in an electronic environment and provides little, if any, protection to PHI. Serious consideration should be given to its deletion.

7.2 *Audits*

Subsections 4(1), (4), (5) and (6) of the Regulation provide as follows:

> 4(1) In accordance with guidelines set by the minister, a trustee shall create and maintain, or have created and maintained, a record of user activity for any electronic information system it uses to maintain personal health information.
>
> 4(4) A trustee shall audit records of user activity to detect security breaches, in accordance with guidelines set by the minister.
>
> 4(5) A trustee shall maintain a record of user activity for at least three years.
>
> 4(6) A trustee shall ensure that at least one audit of a record of user activity is conducted before the record is destroyed.

It is understood that Subsection 4(1) compels trustees to ensure that its electronic information systems can create and maintain a RUA. For large electronic information systems that are accessed by multiple trustees with multiple users, the volume of RUA data can become huge and costly to maintain, and in some instances can be so voluminous so as to affect system performance. For example eChart Manitoba maintains terabytes of such data.

Between them, Subsections 4(5) and (6) require that RUAs be maintained for a minimum of the greater of (i) three years and (ii) when an audit of the RUA has been conducted. A practical question arising from this is whether there is any need to maintain the evidence of the audit itself? Once a RUA (or a portion thereof) has been expunged, what record is there that an appropriate audit had been performed on the expunged record? As a result, out of an abundance of caution some trustees maintain the audit records themselves, which only compounds the space storage and consequent performance issues.

Under *The Limitation of Actions Act*, the limitation period for commencing an action for breach of privacy is three years from when the individual becomes aware of the breach. Rarely do people become aware of a breach of their privacy in an electronic information system when it occurs – they most likely become aware when the consequences of the breach occur (e.g., their information is used inappropriately). Plus that Act has a number of provisions that allow for an effective extension of a limitation period. Therefore a prudent trustee will not only maintain the RUA itself for more than three years, it will also maintain the audit logs that show that the RUA was audited and had not disclosed privacy breaches. This prudent practice only contributes to the collection and storage of data, which as mentioned, results not only in the storage of a tremendous amount of data (at some expense to the health care system) but also in adverse impact on the performance of the systems in question.

8. Disclosure Without Consent: Elements of Consent & Limits to Disclosure

8.1 *Health, Social Service or Integrated Program, Service or Benefit*

The manner in which health services are delivered has evolved in the twenty years since PHIA's enactment. This observation underscores the merits of revisiting key provisions in terms of how PHIA organizes itself around common understanding of what is involved in health services delivery. Increasingly, health and social services have moved away from centralized institution-based models towards community-based services and programs that work with individuals though multidisciplinary care coordination that involves the services of multiple partners. For example, this is recognized in part by the provisions of the PCIS Act which use the concept of "service provider", which is broader than what is reflected in PHIA.

PHIA defines health care as:

> "**health care**" means any care, service or procedure
> (a) provided to diagnose, treat or maintain an individual's health,
> (b) provided to prevent disease or injury or promote health, or
> (c) that affects the structure or a function of the body,
> and includes the sale or dispensing of a drug, appliance, device, equipment or other item pursuant to a prescription;

PHIA Paragraph 22(2)(a) permits disclosure of PHI without consent "to a person who is or will be providing or has provided health care…to the extent necessary to provide health care…". Subsection 19.1(4) provides:

> 19.1(4) Consent must be express, and not implied, if
> (a) a trustee makes a disclosure to a person that is not a trustee; or
> (b) a trustee makes a disclosure to another trustee, but the disclosure is not for the purpose of providing health care or assisting in providing health care.

These provisions all refer to the provision for "health care". Any disclosure made for purposes of providing "social services" (to the extent that they are not also "health care" as defined) must have the individual's express consent. This makes the administration and delivery of these multidisciplinary services programs cumbersome. As an example, the "Block by Block" Initiative and the "Housing, Supports & Service Integration" include multiple service providers, such as the WRHA and Employment Income Assistance (EIA), who coordinate services for the purposes of helping to ensure sustainable housing for a highly marginalized population. Referrals for these programs are delayed or hindered as service providers must ensure documentation of express

consent before making a referral based on observed fit and need between client and program. This means that the disclosure of PHI without consent of the individual to other entities that do not provide health care to the individual, such as Manitoba Housing, Employment and Income Assistance, Main Street Project, Siloam Mission, and the Salvation Army, is significantly restricted. By way of example, the WRHA can only share basic demographic PHI about an individual who would benefit from inclusion in integrated programs. There is no ability to provide general PHI such as diagnosis, treatment requirements, admissions, etc., or to share PHI beyond demographics, at the point in time where eligibility for the program is being determined.

Paragraph 22(2)(g.2) of PHIA provides:

> 22(2) A trustee may disclose personal health information without the consent of the individual the information is about if the disclosure is
> (g.2) for the purpose of determining or verifying the individual's eligibility for a program, service or benefit, if the information disclosed is limited to the individual's demographic information;

As the phrase "program, service or benefit" is not defined in PHIA, it is unclear whether it would extend beyond health care programs, and to other government entities or non-government organizations. It is currently being read by the WRHA and others as a program, service or benefit in the health care field only.

It is recommended that:

- PHIA more clearly define "program, service or benefit" to include multidisciplinary service partnerships such as those just discussed;
- participation in or application for such a program be understood as implied consent to share PHI to the extent necessary to provide the service under PHIA; and
- PHIA permit that referral to such programs may require disclosure of more than demographic information.

For example, New Brunswick's *Personal Health Information Privacy and Access Act* provides:

> 38(1) A custodian may disclose personal health information relating to an individual without the consent of the individual if the disclosure is
> (a) for the purpose of determining or verifying the eligibility of the individual to receive health care or related goods, services or benefits provided under an Act of the Legislature or the Parliament of Canada and funded in whole or part by the Province or the Government of Canada,

(d.1) if the custodian is a public body, for the purpose of planning or delivering an integrated service, program or activity,
(d.2) if the custodian is a health care provider, for the purpose delivering an integrated service program or activity,

That Act defines "integrated service, program or activity" as "an integrated service, program or activity as defined in the Right to Information and Protection of Privacy Act", which in turn means "an authorized service, program or activity that provides support or assistance with respect to the mental, physical or social well-being of individuals through

(a) a public body and one or more other public bodies working cooperatively, or
(b) one public body working on behalf of one or more other public bodies."

It is recommended that Manitoba consider similar language for inclusion in PHIA while also recognizing that in Manitoba, integrated services are often delivered through partnerships that include not just trustees but also health and social services agencies. For example, using a defined term such as:

> "**health, social service or integrated program, service or benefit**" means a service, program or benefit provided under an Act of Manitoba or Canada or a service, program or benefit that provides support or assistance with respect to the mental, physical or social well-being of an individual through the involvement of one or more entities funded in whole or in part by the Government of Manitoba or Canada, by a Regional Health Authority or by a municipality.

Should social and integrated programs be acknowledged in PHIA, consideration should also be given to whether to include such programs in the term "trustee" or "agent" as discussed in Section 1.1 of this Report.

8.2 *Disclosure to a Person Who Has Provided Health Care*

PHIA Paragraph 22(2)(a) allows disclosure to a person who "has provided health care" but only "to the extent necessary to provide health care". A problem arises with this language: the person has provided health care in the past, but disclosure may be made only for providing health care in the present time. Common examples of persons who provided health care and who may now require access to PHI are: non-referring family physicians requesting death certificates or confirmations from a hospital; referring physicians inquiring about the current health state; a desire by care providers to know the outcome of their own health care choices for a given patient for purposes of their own professional learning.

For the purposes of providing clarity on this matter it is recommended that Paragraph 22(2)(a) be amended to allow persons who provided health care in the past to access PHI for the purpose of completing their records or for assessing the quality of the health care they provided.

8.3 *Disclosure of PHI Already in the Public Domain*

Where an individual has freely disclosed his or her PHI into the public domain, it is often their expectation that a trustee may then equally respond to questions from third parties about that patient and PHI. These third parties are often family members, friends, advocates, etc. However, PHIA currently does not allow this, so that trustees are constrained in what they can say without the express consent of the individual. While frustrating, it is recognized that there are important issues such as whether the individual had in fact been the source of the PHI, the PHI is the individual's to deal with as the individual sees fit, any discussion of the details of a patient's case may result in disclosure of more PHI than the individual had intended, and so on. However, when the information concerns a trustee's services or programs, it is often in the public interest to have accurate information available about those services and programs.

It is recommended that further consideration be given to the foregoing, and that at least PHIA Subsection 22(2) be amended to allow for disclosure of PHI without the consent of the individual where the trustee's disclosure is limited to the amount reasonably necessary to correct any inaccurate information about a service or program of the trustee that had previously been disclosed by the individual, provided that:

- the trustee reasonably believes that the PHI had already been disclosed to the public by the individual, and
- the trustee does not, without consent, disclose more PHI than had already been disclosed by the individual.

8.4 *Disclosure of Information about a Deceased Individual*

Trustee obligations remain consistent for any record containing PHI. This includes the PHI of deceased individuals. The WRHA as trustee regularly receives requests from family members for the PHI of deceased individuals. There is no exhaustive and reliable source of truth for a trustee to confirm death. If death did not occur while the patient was being cared for by the trustee or in the trustee's facility, and if the family does not produce a death certificate, the trustee has only the Client Registry system to look to, which discloses on a delayed basis only reported deaths that occur in Manitoba. Without a separate disclosure directive on the patient's chart about who may or may not receive information in the event of a death – a common occurrence – a trustee must look to the provisions of PHIA to determine whether disclosure to grieving family is permissible.

PHIA provides that:

> 22(2) A trustee may disclose personal health information without the consent of the individual the information is about if the disclosure is
> (d) to a relative of a deceased individual if the trustee reasonably believes that disclosure is not an unreasonable invasion of the deceased's privacy;

The above provision applies a significant expectation on the trustee to determine what may or may not be unreasonable to an individual they may have never met for disclosure to family they do not know. This leads trustees to look for greater certainty and input from someone known to have had a close personal relationship with that individual. In other words, trustees in practice seek consent where in law they may not have to. PHIA Section 60 does address who may exercise the rights of an individual, including for consent to disclose PHI, as follows:

> 60(1) The rights of an individual under this Act may be exercised
> (a) if the individual is deceased, by his or her personal representative.
>
> 60(2) If the trustee reasonably believes that no person listed in subsection (1) exists or is available, the adult person listed first in the following clauses who is readily available and willing to act may exercise the rights of an individual who lacks the capacity to do so:
> (a) the individual's spouse, or common-law partner, with whom the individual is cohabiting;
> (b) a son or daughter;
> (c) a parent, if the individual is an adult;
> (d) a brother or sister;
> (e) a person with whom the individual is known to have a close personal relationship;
> (f) a grandparent;
> (g) a grandchild;
> (h) an aunt or uncle;
> (i) a nephew or niece.

So the trustee is put into the position of:

- confirming that the individual is dead,
- making an assessment of what may be appropriately disclosed, and
- identifying to whom disclosure may be made,

sometimes in circumstances where the trustee has no firsthand knowledge.

This is a difficult and highly stressful circumstance for all involved, including and especially grieving family members who may be dealing with their own conflict. The provision of Paragraph 22(2)(d) may be very reasonable when the trustee is a family doctor who has an established relationship with the deceased (and possibly with the family) making a determination about what may be reasonable disclosure. It is far more complicated when the trustee is an organization with the lack of familiarity discussed above.

Other jurisdictions, notably Nova Scotia, have provided for more detailed instruction about how PHI of deceased individuals may be managed, as follows:

> 40(1) A custodian may disclose personal health information about an individual who is deceased, or is believed to be deceased,
> (a) for the purpose of identifying the individual;
> (b) for the purpose of informing any person whom it is reasonable to inform that the individual is deceased or believed to be deceased;
> (c) to a spouse, parent, sibling or child of the individual if the recipient of the information reasonably require the information to make decisions about the recipient's own health care or the recipient's children's health care and it is not contrary to a prior express request of the individual; or
> (d) for carrying out the deceased person's wishes for the purpose of tissue or organ donation.
>
> (2) Where an individual is deceased, personal health information may be disclosed by a custodian to
> (a) a family member of the individual; or
> (b) to another person if the custodian has a reasonable belief that the person has a close personal relationship with the individual,
>
> if the information relates to circumstances surrounding the death of the individual or to health care recently received by the individual and the disclosure is not contrary to a prior express request of the individual.

The Yukon's *Health Information Privacy and Management Act* is considerably more concise in their provision, stating simply that:

> 47 If an individual is deceased, any right or power conferred on an individual by this Act may be exercised by the deceased's personal representative if the exercise of the right or power
> (a) relates to the administration of the deceased's estate; or
> (b) relates to a claim under a policy of insurance in which a benefit is payable upon the death of the deceased.

It is recommended that Manitoba give serious consideration to adopting language similar to the Nova Scotia provisions, so as to provide all trustees with better guidance on what may be disclosed, the circumstances of permitted disclosures, and to whom.

8.5 *Disclosure to Family*

PHIA provides that:

> 23(1) If an individual is a patient or resident in a health care facility, or is receiving health care services from a trustee at home, the trustee may disclose personal health information about the individual to an immediate family member, or to anyone else with whom the individual is known to have a close personal relationship, if
> (a) the disclosure is about health care currently being provided;
> (b) the disclosure is made in accordance with good medical or other professional practice; and
> (c) the trustee reasonably believes the disclosure to be acceptable to the individual or his or her representative.

Also as previously discussed, when the trustee is a hospital or a RHA, knowing what may or may not be reasonably acceptable to individuals who may be unable to speak for themselves may require some guesswork. In an effort to provide greater certainty and direction, some other jurisdictions have included more permissive language in the provisions regarding disclosure to family. For example, Nova Scotia's legislation provides:

> Disclosure of general information
> 37 A custodian has the discretion to disclose personal health information about an individual to
> (a) family members of the individual; or
> (b) to another person if the custodian has a reasonable belief that the person has a close personal relationship with the individual, if the information is given in general terms and concerns the presence, location, and general condition of the individual on the day on which the information is disclosed and the disclosure is not contrary to the express request of the individual.

The Nova Scotia provision is helpful in that it grants the custodian the ability to make judgement calls (e.g., Nova Scotia's "has the discretion" and "has a reasonable belief" v. Manitoba's "may disclose" and "is known to have".) The ability to disclose to family members is qualified by Paragraphs 23(1)(a), (b) and (c), whereas the reference in the Nova Scotia legislation to family members is not qualified. It is recommended that we take a step back and engage in a discussion on what is appropriate disclosure to family members.

The conflict between a patient's privacy rights (with the obligation on the trustee to maintain and protect that privacy) and the desire of family members to gain more knowledge about the health condition and the treatment of a loved one is a very difficult one for all concerned. PHIA is built on a privacy rights model – it enshrines the legal right of an individual to keep all of their PHI confidential (and in the words of some, the right to be left alone). PHIA allows a trustee to disclose PHI only with the individual's consent, or without consent in the limited circumstances set out in PHIA. On the other hand, family members are often advocates and supports for their loved one, and in some cases are care givers in their own right. They seek access to the individual's PHI in part out of concern and in part in continuation and support of their advocacy and support roles. This would be a move to a "patient's best interests" model, and should it occur, such a change needs to be expressly acknowledged.

Ideally, the patient in each case will provide direction and hence consent on what PHI may be disclosed to family members, and to which family members. Trustees should take the opportunity to discuss with patients what disclosure they should consider consenting to. But sometimes the patient is not able or does not have an opportunity to give such direction and consent. Sometimes the patient directs that there is to be no disclosure, and the family may strongly disagree with the direction given by the patient. And from the family's perspective, this is usually a time of stress as they deal with the condition or circumstances that put their loved one in the hospital.

The WRHA is not recommending specific changes to PHIA on the issue. But it does acknowledge that this is a source for ongoing difficulties, both for trustees and for family members, and that there is an opportunity here to engage stakeholders in a public discussion of what is appropriate.

8.6 *Disclosure about Patient's Condition*

Subsection 23(2) states that:

> As long as disclosure is not contrary to the express request of the individual or his or her representative, a trustee may disclose to any person the following information about an individual who is a patient or resident of a health care facility:
> (a) the individual's name;
> (b) the individual's general health status, described as critical, poor, fair, stable or satisfactory, or in terms indicating similar conditions;
> (c) the individual's location, unless disclosure of the location would reveal specific information about the health of the individual.

This limits disclosure to only current patients or residents of a facility. In the event that a patient has been transferred to a different facility or to a PCH, it does not permit the first facility to

advise callers and visitors of the patient's new facility or location, or that the patient has died. This is a circumstance that is frequently frustrating to concerned callers and to staff.

It is recommended that the language in Subsection 23(2) be amended to include as permitted disclosures, subject to the express request of the individual:

- whether the individual has been discharged from the facility or has died
- whether the individual has been transferred to another facility, and the name of that facility, if known.

9. Disclosure Outside of Manitoba

The export of PHI to a physician in another province for purposes of a consultation or second opinion has occurred for years. This usually involves sending a copy of the patient's paper chart and diagnostic results. This practice is increasing and will soon, if not already, involve electronic data and transmission. For example, work is underway on a project to engage Ontario physicians to provide primary pathology services (the Multi-Jurisdictional Telepathology project (MJT)). Increasingly, patient charts and results are sent electronically, and the MJT will be totally electronic. PHIA is silent on the export of PHI to another province, and no regulation on this has been enacted, and hence there is no guidance given on what steps must be taken to ensure the confidentiality of the PHI while in the other jurisdiction.

While the electronic sharing of digital PHI is somewhat in its infancy, we need to anticipate the time when cross-border sharing and accessing of PHI will be considered routine, to accommodate the utilization of extra-provincial resources and expertise, and to accommodate the interests and needs of people who live in one province or territory and receive health care in another.

The ideal solution to extra-provincial sharing of PHI is to create a "community of trust" amongst all of the provinces and territories, whereby all jurisdictions are satisfied that there are adequate protections in place (legal and practical) which ensure the continued privacy and confidentiality of PHI regardless of where it may be located. But until that is achieved, it is desirable for Manitoba's PHIA to accommodate what is already occurring, and will increasingly occur, in a manner that ensures the protection of the Manitobans' PHI to Manitoba standards. Having said that, serious consideration will be required at some point on how health care providers in other jurisdictions (e.g., Kenora and Creighton) may access the PHI of their patients maintained in Manitoban electronic information systems.

Cross-jurisdictional issues are not limited to those that cross Manitoba's borders. The Government of Canada, through its First Nations and Inuit Health Branch (FNIHB), is responsible for providing health care to many First Nations and Inuit people who often reside in northern Manitoba. FNIHB operates nursing clinics across northern communities and a hospital in Hodgson. FNIHB patients will often receive health care services in Winnipeg, so that access by personnel in FNIHB facilities to their patients' PHI stored in Manitoba electronic information systems (especially eChart Manitoba) is required. Because the Government of Canada takes the position that it is not subject to PHIA, this has been handled by the imposition by contract of pertinent PHIA obligations on FNIHB and its personnel. If and when FNIHB starts to transition to First Nations and Inuit organizations the conduct of their health services, the whole issue of the application of PHIA will need to be revisited once again.

So the most immediate issue for consideration is the current practice of "exporting" PHI to health care providers located in another province or territory. The issues for PHIA are:

- May this occur? PHIA currently does not allow for it, but it also does not prohibit it. It is desirable to give trustees the comfort of knowing that the practice is expressly allowed by PHIA.

- The protections and assurances that the disclosing trustee is required to ensure are in place in the receiving jurisdiction – is it sufficient for the trustee to satisfy itself that it has taken sufficient steps pursuant to Section 18 of PHIA by reviewing the privacy laws of the receiving jurisdiction, and by imposing the pertinent PHIA obligations on the extra-provincial recipient by contract? It may be sufficient to provide in PHIA that the exporting trustee is reasonably satisfied that the confidentiality of the PHI will be protected to the same extent as required by PHIA.

- The circumstances in which the practice is permitted – for example, are there circumstances where exporting of PHI would not be allowed? (None are being asserted here.) Is patient express consent always required? While requiring express consent each time might seem sensical where exporting PHI in an unusual "one-of" transaction, such as for a consultation or second opinion, this in fact may become a routine transaction under projects such as the MJT where whether a Manitoba or Ontario pathologist receives the PHI is not necessarily known until the immediate need to export (e.g., due to workload that week) is identified. As long as there is a reasonable assurance that protections are in place for the PHI while in another province or territory, there should not be any undue risk to the PHI that would require the step of express consent each time.

Ontario's *Personal Health Information Protection Act* attempts to deal with this by providing:

> 50(1) A health information custodian may disclose personal health information about an individual collected in Ontario to a person outside Ontario only if,
> (a) the individual consents to the disclosure;
> (b) this Act permits the disclosure;
> (c) the person receiving the information performs functions comparable to the functions performed by a person to whom this Act would permit the custodian to disclose the information in Ontario under subsection 40 (2) or clause 43 (1) (b), (c), (d) or (e);
> (d) the following conditions are met:
> (i) the custodian is a prescribed entity mentioned in subsection 45 (1) and is prescribed for the purpose of this clause,
> (ii) the disclosure is for the purpose of health planning or health administration,

(iii) the information relates to health care provided in Ontario to a person who is resident of another province or territory of Canada, and
(iv) the disclosure is made to the government of that province or territory;

(e) the disclosure is reasonably necessary for the provision of health care to the individual, but not if the individual has expressly instructed the custodian not to make the disclosure; or

(f) the disclosure is reasonably necessary for the administration of payments in connection with the provision of health care to the individual or for contractual or legal requirements in that connection.

(2) If a health information custodian discloses personal health information about an individual under clause (1) (e) and if an instruction of the individual made under that clause prevents the custodian from disclosing all the personal health information that the custodian considers reasonably necessary to disclose for the provision of health care to the individual, the custodian shall notify the person to whom it makes the disclosure of that fact.

It is recommended that Manitoba consider adopting a similar provision for PHIA.

10. Disclosure for Research

Health research is a valuable aspect of the health care sector. It informs medical practices and leads to improvements in health care and health care results. It contributes to the high level of training and education for students, interns, residents, etc., in our health care system. The fact that Winnipeg is a significant medical research centre maintains, and continues to attract to the WRHA, a high calibre of physicians and other health care professionals. It is an important economic engine itself for the Winnipeg economy. So with all of the positive reasons, if not imperatives, for encouraging health research, it is vital that at all times the privacy of the PHI of Manitobans is appropriately protected.

Many University-affiliated research scientists who do not have clinical credentials (MD, BN, MN, etc.) and are not WRHA employees also perform health research using PHI. Therefore, the term "researcher" can mean a WRHA employee, a non-WRHA employee such as a University-employed researcher, and clinician-researchers who may have a University affiliation and have an independent contractor relationship with the WRHA.

There are three major parties in the research approval process:

1. The trustee who maintains the copy of the PHI which the research project wishes to utilize – the trustee bears the full scope of responsibilities set out in PHIA, including seeing to the compliance by the researcher with the terms of the research agreement;

2. The researcher who proposes the research project and will be responsible for leading the research for compliance with the research agreement entered into – it is important to note that the obligations of the researcher do not involve compliance with PHIA, but instead compliance with the contractual obligations set out in the research agreement; and

3. The review committees, being the health information privacy committee and the institutional research review committees – their role is limited to making the four determinations set out in PHIA Subsection 24(3).

There are a number of challenges with the current regime set out in PHIA Section 24.

10.1 Role of Trustee

PHIA Section 24 outlines responsibilities of trustees to ensure observance of appropriate considerations and safeguards for the protection of PHI prior to disclosure of same for research purposes. Despite Subsection 24(3) of PHIA, in practice, the responsibility for ensuring the

protection of privacy falls upon the trustee, such as vetting of research requests for compliance with Subsection 24(3), ensuring that the PHI used in research is the minimum amount necessary for the purpose and that there are sufficient safeguards in place to protect the data, to bind the researcher to an agreement and to ensure that the protocols outlined in the agreement are being followed. The trustee is reliant upon clear and accurate information being provided by the researcher in order to ensure compliance with its obligations under PHIA.

Ultimately, responsibility for whether a research project complies with PHIA is upon the trustee. There is no independent obligation under PHIA for the researcher to comply with PHIA, just the contractual obligations set out in the research agreement. It is recommended that researchers have a direct obligation to comply with PHIA, both in terms of meeting all of the requirements of Section 24 and the protection of PHI which comes into the researcher's possession in connection with the research project.

For example, contrast PHIA Section 24 with the *E-Health (Personal Health Information Access and Protection of Privacy) Act* of British Columbia which places the onus on the researcher to provide the information (equivalent to the information required by the trustee in PHIA Subsection 24(3)) as follows:

> 14(1) A person may request protected information for a health research purpose only by submitting to the data stewardship committee
> (a) a request in the form and in the manner required by the data stewardship committee, and
> (b) information required by the data stewardship committee for the purposes of evaluating the request.
> (2) The data stewardship committee may approve the request if both of the following apply:
> (a) in the case of a request to disclose personal health information, all of the requirements set out in subsection (2.1) are met;
> (b) in the case of a request to disclose protected information outside Canada, there is express consent, in writing, to the disclosure from each person who is the subject of the protected information.

In so doing, BC shifts the accountability of ensuring adequate and accurate information to the person submitting the information. This approach helps to address the current imbalance of accountabilities whereby researchers, who have no such legislated accountabilities in Manitoba, frequently express frustration at trustee efforts to obtain the information required for appropriate review of research submissions in keeping with current trustee obligations.

We recommend that Manitoba consider adoption of similar provisions.

10.2 Certainty of Roles

In addition to the standards for approval outlined in Subsection 24(3) and provided above, PHIA authorizes two distinct types of bodies as having the authority to approve disclosure of PHI for research as follows:

> 24(2) An approval may be given by
> (a) the health information privacy committee established under section 59, if the personal health information is maintained by the government or a government agency; and
> (b) an institutional research review committee, if the personal health information is maintained by a trustee other than the government or a government agency.

PHIA Section 24 is written largely from the consideration of paper-based records and presupposes a circumstance in which the trustee has sole access to and control of data, which it may then disclose when conditions under Section 24 are met. These provisions are highly responsive to the experience of the Government of Manitoba as a trustee with stores of administrative health data (secondary data) and of data sourced from and disclosed by frontline trustees (primary data). In these circumstances, the trustee can limit who may receive data and in which format, and in so doing ensure compliance with the conditions outlined in PHIA Section 24. But these provisions are considerably less responsive to circumstances where trustees are RHAs that employ other health services professionals (most of whom are trustees in their own right) who already have direct access to the data for primary purposes, which data they would seek access to for the secondary purpose of research. In other words, in the case of research proposals involving the WRHA, the researcher likely has access to the PHI already and sees the Section 24 process as an unnecessary impediment. This, amongst other things, further diminishes the ability of the WRHA to insist upon full compliance with the information submission requirements under Section 24.

In addition, the WRHA encompasses both devolved and non-devolved sites, all of which are authorized to have, and over time have developed, their own review processes in compliance with Paragraph 24(2)(b). Increasingly, research proposals are becoming more sophisticated and complex wanting to look at interactions amongst increasingly large patient pools across sites, as well as for information maintained in electronic data systems of which the WRHA is the trustee.

These combined circumstances of increasing sophistication of research projects, increasing independent access to valuable digitized data, multiple access and review points for approval, misunderstandings about authorities and accountabilities of trustees and researchers, and imbalance of accountability for ensuring PHIA compliance between trustees and researchers, have created a cumbersome research environment in Manitoba that is not as supportive or as responsive to valuable health research as would be preferred.

In order to move forward, we recommend steps to address these complexities including:

- the addition of some key definitions
- the addition of provisions to more clearly outline authorities of trustees and to provide greater parity of accountabilities by all parties.

We already discussed above the proposed amendment of Paragraph 22(d)(ii) so as to change the reference to "research". This would greatly assist in the WRHA resisting efforts to use that paragraph as a way of avoiding Section 24.

So as to designate an individual who is responsible for ensuring compliance with Section 24, PHIA in general, and the research agreement, and who is currently referred to in Section 24 as "a person", it is recommended that the concept of "principal investigator" be introduced, defined as follows:

> **"principal investigator"** means the individual leading a research project who seeks the approval of the research project required under Section 24 and who enters into the research agreement in respect of an approved research project;

The principal investigator then should be made responsible for meeting the approval requirements set out pursuant to Section 24, for compliance with the research agreement, and for ensuring generally that the PHI is protected as required by PHIA and by the research agreement. Accordingly, the principal investigator should be expressly included in Subsection 63(3).

The goal here is in part to provide clarity between the role of the trustee as having the responsibility and obligation to authorize disclosure and the role of the principal investigator going forward for the conduct of the research project and the protection of PHI. The trustee's capacity to compel compliance with research agreements is often dependent upon the capacity to remove access to data. This capacity is minimized when principal investigators already have independent access to data as discussed above, though not necessarily access in a PHIA-compliant manner.

10.3 Regional Role

In addition, to address the current administrative impasse experienced by a principal investigator wishing to conduct multi-site research or that requires access to PHI in electronic data systems maintained by the WRHA, it is recommended that PHIA recognize a specific role for RHAs to review and approve such projects on a regional basis as opposed to obtaining site approvals on a one-by-one basis. It is proposed that the following definition be introduced into PHIA:

> **"regional research review committee"** means a committee formally established by a Regional Health Authority
>
> a) to ensure compliance with subsection 24(3),
> b) to review the efficacy and scientific and ethical value of a research proposal involving human subjects or involving the collection, use and/or disclosure of personal health information, and
> c) to ensure that the person proposing the research has adequate safeguards in place to protect the confidentiality of personal health information;

and that Subsection 24(2) be amended to add:

> a regional research review committee, if the personal health information is maintained by a Regional Health Authority or by more than one organization or facility (other than the government or a government agency) located in the corresponding Health Region.

The inclusion of a definition and recognized role for "regional research review committee" is recommended to stress the importance of differentiating the role and purpose of a RHA from that of a hospital in terms of practical considerations and functions with regards to research applications review and approval. Both RHAs and hospitals are considered public bodies and trustees. Increasingly, planning, analysis and research, for example, involve the data resources of multiple sites within a RHA. In addition, increasingly, electronic health record systems are being operationalized and maintained regionally. Distinguishing the role of a RHA with these systems would help provide role clarity as well as accountability and authority to ensure same. It would further significantly cut back on both the time required for multiple reviews for projects of this nature as well as the current uncertainty by sites and researchers alike about what may be required to obtain PHI for research where the project involves data sourced from more than one site or facility within a single RHA.

The use of "collection, use and/or disclosure of personal health information" in the above definition provides clarity as to what must be considered approving access to PHI held by a trustee, as well as stresses that research involving PHI entails more than just access to records.

A well-rounded example of how mutuality of accountability may be represented in law may be found in Nova Scotia's *Personal Health Information Act*, which provides more detailed obligations of both researchers requesting data and trustees evaluating requests for disclosure as follows:

> 56 A custodian may disclose personal health information about an individual to a researcher if the researcher
> (a) submits to the custodian
> (i) an application in writing,
> (ii) a research plan that meets the requirements of Section 59, and

(iii) a copy of the submission to and decision of a research ethics board that approves the research plan; and

(b) enters into the agreement required by Section 60.

57 A custodian may disclose personal health information about an individual to a researcher without the consent of the subject individual if

(a) the researcher has met the requirements in Section 56;

(b) a research ethics board has determined that the consent of the subject individuals is not required;

(c) the custodian is satisfied that

(i) the research cannot be conducted without using the personal health information,

(ii) the personal health information is limited to that necessary to accomplish the purpose of the research,

(iii) the personal health information is in the most de-identified form possible for the conduct of the research,

(iv) the personal health information will be used in a manner that ensures its confidentiality, and

(v) it is impracticable to obtain consent; and

(d) the custodian informs the Review Officer.

58 A custodian may prescribe forms for use by researchers for

(a) an application under clause 56(a)(i);

(b) a research plan under Section 59; and

(c) a disclosure agreement under Section 60.

59(1) Before commencing research, a researcher seeking to conduct research utilizing personal health information shall submit a research plan to a research ethics board.

(2) The research plan must be in writing.

(3) In order to meet the requirements for a custodian under this Act, the research plan must include

(a) a description of the research proposed to be conducted;

(b) a statement regarding the duration of the research;

(c) a description of the personal health information required and the potential sources of the information;

(d) a description as to how the personal information will be used in the research;

(e) where the personal health information will be linked to other information, a description of the other information as well as how the linkage will be conducted;

(f) where the researcher is conducting the research on behalf of or with the support of a person or organization, the name of the person or organization;

(g) the nature and objectives of the research and the public or scientific benefit anticipated as a result of the research;

(h) where consent is not being sought, an explanation as to why seeking consent is impracticable;
(i) an explanation as to why the research cannot reasonably be accomplished without the use of personal health information;
(j) where there is to be data matching, an explanation of why data matching is required;
(k) a description of the reasonably foreseeable risks arising from the use of personal health information and how those risks are to be mitigated;
(l) a statement that the personal health information is to be used in the most de-identified form possible for the conduct of the research;
(m) a description of all individuals who will have access to the information, and
  (i) why their access is necessary,
  (ii) their roles in relation to the research, and
  (iii) their qualifications;
(n) a description of the safeguards that the researcher will impose to protect the confidentiality and security of the personal health information;
(o) information as to how and when the personal health information will be destroyed or returned to the custodian;
(p) the funding source of the research;
(q) whether the researcher has applied for the approval of another research ethics board and, if so, the response to or status of the application; and
(r) whether the researcher's interest in the disclosure of the personal health information or the conduct of the research would potentially result in an actual or perceived conflict of interest on the part of the researcher.

60(1) Where a custodian discloses personal health information to a researcher, the researcher shall enter into an agreement with the custodian to adhere to the requirements in subsection (2).

(2) An agreement referred to in subsection (1) must include a commitment by the researcher
(a) to comply with any terms and conditions imposed by a research ethics board;
(b) to comply with any terms and conditions imposed by the custodian;
(c) to use the information only for the purposes outlined in the research plan as approved by a research ethics board;
(d) not to publish the information in a form where it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual;
(e) to allow the custodian to access or inspect the researcher's premises to confirm that the researcher is complying with the terms and conditions of this Act and of the agreement between the custodian and the researcher;
(f) to notify the custodian immediately and in writing if the personal health information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification;
(g) to notify the custodian immediately and in writing of any known or suspected breach of the agreement between the custodian and the researcher; and

(h) not to attempt to identify or contact the individuals unless the custodian or researcher has obtained prior consent by the individuals.

The measures outlined in the Nova Scotia legislation mirror the established nationally recognized best practice standards already employed in Manitoba as elsewhere for review, approval and disclosure of PHI for research. Enshrining these considerations in law would not only empower trustees to continue in their best efforts to ensure privacy protection while supporting valuable research, it would also send a powerful message to Manitobans that trustees and principal investigators can be entrusted with their PHI. It is recommended that Section 24 be revised, using the quoted Nova Scotia provisions as a guide for what a strengthened research provision may encompass.

10.4 Limitation for Projects Requiring Direct Contact with Individuals

PHIA Subsection 24(5) authorizes trustees to disclose individuals' names and addresses for the purposes of health research without consent.

This practice has at times resulted in individuals being upset that their care services provider disclosed their PHI to an external researcher without their permission. It stands to reason that even though the disclosure is demographic information only, when coupled with the exact nature or field of research, the demographic information by virtue of inclusion in subject pool for a stated research objective further discloses something about that individual's health circumstance.

In Manitoba, MHSAL and the WRHA have adopted a process whereby for research approved under Subsection 24(3) that requires direct contact with individuals, rather than disclosing demographic information, the trustee undertakes the process of mailing an invitation to participate in the research. This involves a cover letter of assurance that no PHI has been disclosed, participation is strictly voluntary, and that health services would be in no way affected by a decision not to take part in the research. This process has worked well in Manitoba as elsewhere.

We recommend that PHIA consider amending the language in Subsection 24(5) by the addition at the end thereof the following:

> … and the disclosure does not otherwise reveal anything specific about the individual's health. Where the research project is about a specific health condition or circumstance, so that disclosing an individual's name and contact information may disclose information about that individuals' health condition or circumstance, the trustee may either by itself or through the services of an information manager contact those individuals to invite their participation in the research project.

11. Minors

PHIA Subsection 60(1) provides that the rights of a minor under PHIA may be exercised by a parent or guardian if the minor does not have the capacity to make health care decisions.

While likely intended as an enabling provision, this creates problems in that it establishes a presumption that all minors can exercise their PHIA rights unless it can be shown that the minor lacks the capacity to make health care decisions. This raises at least three issues:

1. Where a minor asserts his or her PHIA rights, the presumption applies until shown otherwise. If Canadian courts are prepared to consider someone as young as 12 years to be a "mature minor" capable of making his or her own health care decisions, a trustee who does not have direct familiarity with the minor is not in a position to rebut the presumption and certainly must be careful where the minor is 12 or older.

2. Unless the presumption is rebutted, do the parents of the minor have any entitlement to access the minor's PHI or to consent to its use and disclosure? There is nothing in PHIA that deals with this. Presumably any parent wanting to access a child's PHI must first rebut the presumption of capacity under Subsection 60(1).

3. Again, unless the presumption is rebutted, a minor can direct under Paragraph 22(2)(a) that his or her parents not be given access to the minor's PHI.

When the trustee is a family physician with direct experience with the minor and/or family, making the determination of maturity may be based on empirical knowledge of the individuals involved. The operationalization of this requirement becomes more abstract to health information staff who may never have had direct contact with the minor and have no capacity to determine the level of maturity when requests for access to information maintained in health records systems are made. It also often requires that trustees take into account the circumstances and the level of sensitivity of information being requested.

This level of uncertainty places an undue burden on trustees and on frontline staff when processing requests for access to the PHI of minors by their parents or guardians. To balance the apparent rights of minors with the needs of parents, standard policy processes are developed to require individual consent for any and all requests for PHI belonging to minors beyond a specified age (for example, eChart Manitoba has set the age at 12). Such processes place front line staff in the firing line of angry parents without the benefit or support of clearly articulated legislative authority. The trustee then bears the risk should a disclosure be made that results in a PHIA breach to the minor. The consideration of more or less sensitive data proves

similarly fraught with uncertainty. For example, parents frequently request their child's immunization records for a variety of purposes and this information is commonly understood as being relatively low risk. However, there has been an incident where disclosing this information also disclosed an HPV vaccine, something the minor would have preferred to keep private. Disclosure of immunization records also bear the risk of disclosing a current address to a non-custodial parent for which there was a non-contact order (not documented on the chart). Had consent been mandatory neither of these circumstances would have occurred.

It is strongly recommended that PHIA take measures to address expressly the issues raised, in part by setting an objective standard so as to more clearly define how the privacy rights of minors and access rights of parents under PHIA shall be met. The one province we are aware of that has addressed this is Quebec, which has the following provision:

> The person having parental authority over a minor child 14 years of age or over is not entitled to be informed of or to receive the information concerning the child that is held in the health information banks in the clinical domains or in the electronic prescription management system for medication, unless the child has consented to it.[12]

[12] http://www.dossierdesante.gouv.qc.ca/en/fichier/Act-respecting-the-sharing-of-certain-health-information.pdf

12. Disclosure to Archives

PHIA does not address authority to disclose historical records containing PHI for archival purposes. Therefore a trustee remains liable for any data containing PHI *ad infinitum* until it is destroyed or erased. Absent clear provisions for transfer, it is unclear that custody and control may shift from one trustee to another, such as for historical data to archives for example. It is recommended that PHIA consider provisions for the disclosure of PHI to archival records and develop provisions for the maintenance, access and disclosure of same whereby a patient record is determined to have reached a predetermined level of maturation and/or has some historical significance.

PHIA does not provide for the destruction or erasure of PHI, other than to require trustees under Subsection 17(1) to establish a policy concerning the retention and destruction of PHI. There are of course a number of considerations regarding when it is appropriate or advisable to destroy PHI. One is *The Limitation of Actions Act.* Another is that PHI is valuable for more than just providing health care to the patient – it can be, and is, used at later times to help evaluate the performance of health care professionals and the delivery of health care, and to conduct research into public health concerns. And ultimately, it may acquire historical significance. Sole medical practitioners may have a patient-centric focus, whereas larger organizations such as RHAs and the Government of Manitoba have the additional larger scope (time wise) considerations as well.

This may not be of consequence for current paper records as trustees have developed destruction policies in accordance with PHIA. It is relevant however for both historical paper records maintained by longstanding trustees such as the Society for Manitobans with Disabilities, St. Amant Centre, historical hospital records, etc., who have no alternative currently but to destroy potentially historically valuable information, records such as those evaluated by the Truth and Reconciliation Commission for example. It is also significant in terms of electronic data. Many trustees require clearer policy provisions for the destruction of electronic records.

It is further noted that *The Archives and Recordkeeping Act* (Manitoba) does not address disclosure for research purposes or archival records directly. Whereby collections are known to contain PHI, the records are seen as being in the custody and control of a government of Manitoba if disclosed to the Government of Manitoba and, as such, subject to review and approval by the Health Information Privacy Committee.

For example, FIPPA provides that

> 48 The head of a public body or the archives of a public body may disclose personal information in a record that is more than 100 years old.

Saskatchewan makes a distinction between archival records and those currently maintained by trustees by incorporating provisions in the *Saskatchewan Archives and Public Records Management Act* for research involving archival records containing PHI as follows:

> 29(1) In this section:
> (3) Personal health information that is obtained from or on behalf of a trustee, person, body or organization mentioned in subsection (2) and that is under the care, control or custody of the Provincial Archives of Saskatchewan may be disclosed to a researcher if:
> (a) the Provincial Archivist is satisfied that:
> (i) the purpose for which the personal health information is proposed to be disclosed is not contrary to the public interest and the research cannot be reasonably accomplished using de-identified personal health information; or
> (ii) the release of personal health information would not constitute an unreasonable invasion of privacy;
> (b) the personal health information is in a record that:
> (i) has been in existence for 30 years or more, but less than 75 years, and the Provincial Archivist is satisfied that the disclosure would not constitute an unreasonable invasion of privacy; or
> (ii) has been in existence for 75 years or more; and
> (c) before disclosing the personal health information to the researcher, the researcher enters into an agreement with the Provincial Archivist:
> (i) to use the personal health information only for the purpose set out in the agreement;
> (ii) to not disclose the personal health information except where authorized by law to do so;
> (iii) to not contact the individual who is the subject of the personal health information, directly or indirectly, for any purpose, except where authorized by law to do so;
> (iv) to take reasonable steps to ensure the security and confidentiality of the personal health information;
> (v) to destroy copies of any records containing personal health information in the manner and within the period set out in the agreement;
> (vi) to notify the Provincial Archivist in writing immediately if the researcher becomes aware that any conditions set out in this section or the agreement have been breached; and
> (vii) to allow the Provincial Archivist to access or inspect the researcher's premises to confirm that the researcher is complying with the terms and conditions of this Act and of the agreement.

It is recommended that Manitoba consider the inclusion of provisions for the disclosure and management of archival records containing PHI which include the transfer of trustee obligations to Archives. This measure may serve to preserve historically valuable data for future research.

13. Viewing One's Own PHI

Some of the most common privacy breaches involve health care staff accessing their own PHI. In the WRHA, the most common cause for discipline following random audits is misuse of confidential information systems to look up one's own PHI. Interestingly, PHIA does not expressly address viewing one's own PHI. PHIA Paragraph 63(2)(b) provides that it is an offence without the authority of the trustee if the employee:

> (b) uses, gains access to or attempts to gain access to another person's personal health information; [emphasis added]

The Manitoba Ombudsman has taken the position that accessing one's own PHI is a breach under this provision. The WRHA's position is that making use of work-related access to confidential information systems to look up one's own PHI is a breach of policy, in part as it is not being done to provide health care. Any use by trustees and their employees that is not authorized under Section 21 would be considered a violation and it is unlikely that an employee would need access to their own PHI for a legitimate purpose. Subsection 21(b) however provides that use of PHI may occur with the individual's consent. The question often raised is why can't an employee consent to viewing their own PHI?

It is recognized that looking at one's own PHI being a privacy breach is not intuitive.

This is an important policy position that deserves further consultation and discussion with stakeholders, and we strongly encourage the province to do so. Then PHIA should be amended to clearly reflect the position arrived at.

14. Negligent or Reckless Conduct

PHIA offences by employees, officers, and agents of a trustee are limited to intentional acts, and thereby negligent or reckless conduct is not an offence.

PHIA Subsection 63(2) provides that:

> 63(2) Despite subsection 61(2), a person who is an employee, officer or agent of a trustee, information manager or health research organization and who, without the authorization of the trustee, information manager or health research organization, wilfully
> (a) discloses personal health information in circumstances where the trustee, information manager or health research organization would not be permitted to disclose the information under this Act; or
> (b) uses, gains access to or attempts to gain access to another person's personal health information;
> is guilty of an offence.

A cursory analysis of the WRHA breach documentation database indicates that the most common cause of breaches is not snooping or willful misconduct but rather employee error or inattention.

We recognize that mistakes happen. However, in the context of PHIA training, the PHIA pledge, extensive WRHA policies on protecting PHI, and awareness of poor computer security practices, negligent or reckless conduct by trustees, employees, officers and agents can in certain circumstances be as unacceptable as intentional conduct. The digitization of data allows for the collection, storage or transmission of vast amounts of data in a simple manner. Insecure transmission practices (such as unencrypted emails and email attachments) and storage practices (such as on USB drives with no encryption or password protection) can no longer be treated as incidents of innocent ignorance. Where the trustee/employee/agent reasonably should have known that the practice or act was a violation of Section 18 of PHIA and was likely to result in the unauthorized disclosure of PHI, there should be some accountability for same.

Saskatchewan has taken steps to further strengthen provisions for outcomes to employees when breaches were not necessarily willful but due to improper or careless file management.[13]

[13] Saskatchewan cracks down on health-record snoops, those who abandon files, http://www.winnipegfreepress.com/arts-and-life/life/health/saskatchewan-cracks-down-on-health-record-snoops-those-who-abandon-files-381399021.html

It is recommended that Subsection 63(2) of PHIA be amended to provide as offences where Paragraphs 63(2)(a) and (b) result from:

- willful conduct, or
- negligent or reckless conduct where the person knew, or reasonably ought to have known, the adverse consequences of that conduct.

15. Third Party Acts

PHIA imposes obligations only on trustees and those connected to trustees (their employees, officers, agents, and information managers). Once PHI is disclosed to a non-trustee, whether in accordance with or in violation of PHIA, it no longer acts to protect the confidentiality of that PHI. It is time for serious consideration to be given to holding third parties responsible when they use or disclose PHI with full knowledge that it is PHI and that they are doing so without the individual's consent or other legal authority. For example, is it acceptable that a person acquires PHI through illegal or illicit means, including the misconduct (known to the person) of a trustee? Or is it acceptable for news media to publish the PHI of individuals when they know that it is PHI and was provided to them without the consent of the individuals in question?

This is an issue that deserves serious consideration and consultation to further protect the privacy of Manitobans.

16. Privacy Impact Assessments

Currently in Manitoba, there is no legislated requirement or guidance for when a Privacy Impact Assessment (PIA) is to be performed. In practical terms, PIAs are often done when they are a condition for third party funding (e.g., required by Canada Health Infoway). They are also required under WRHA policy where the creation of a new electronic repository of PHI is proposed, or an existing repository is to undergo a substantive change.

A PIA is a valuable tool that enables:

1) a proposed activity or repository has been closely reviewed for compliance with applicable privacy law (usually PHIA and/or FIPPA), and
2) any risks to privacy and/or confidentiality have been identified and appropriate risk management responses will be put into place.

It is noted that an extensive new form of PIA, and accompanying user guide, were developed a few years ago as a result of extensive effort and consultation by MHSAL, Manitoba eHealth and the WRHA. These have been successfully adopted and have eased the PIA process.

By raising the issue of PIAs in this Report, it is not being recommended that all of the circumstances of requiring PIAs, and their format, be enshrined in legislation. We must be careful of avoiding the creation of inflexibilities and distortions, and of causing the effort that goes into PIAs to be diminished by requiring their completion on a more frequent basis than is currently the case. However, there is perceived value in having guidance in the Regulation as to when a PIA should be performed. For example, Ontario's *Bill 78, Electronic Personal Health Information Protection Act, 2014,* provides in part*:*

> 10. It shall perform, for each system that retrieves, processes or integrates personal health information in the electronic health record, an assessment with respect to,
> (i) threats, vulnerabilities and risks to the security and integrity of the personal health information in the electronic health record, and
> (ii) how each system that retrieves, processes or integrates personal health information in the electronic health record may affect the privacy of the individuals to whom the information relates.

17. Notification of Privacy Breaches

PHIA does not require trustees to notify individuals whose privacy of PHI has been breached.

The WRHA has established protocols that require that individuals be notified whenever there is a reasonable potential of harm as a result of a breach. This includes notification anytime an individual has been directly targeted - or snooped - and/or sufficient levels of their PHI has been breached to place them at risk of harm. Harm includes consideration of physical harm (such as when addresses and access codes are compromised), financial harm (such as risk of identity theft), and psychological/emotional harm (such as due to embarrassment, loss of trust or standing). The decision whether to notify is made by the program in consultation with their privacy officer and with the WRHA Chief Privacy Officer. In other words, an individual is notified when a breach has not been sufficiently and immediately mitigated so as to remove the risk of harm, and always when a person has been directly targeted through snooping.

While in no way diminishing the importance of maintaining the confidentiality and privacy of PHI or the prospect of adverse harm, where the prospect of harm is unlikely or nil, then consideration must also be given to maintaining public confidence in the ability of the health care system to keep their PHI protected. Loss of confidence would have a significant adverse impact on health care.

For example, the Ponemon Institute LLC[14] has published survey results showing that media reports of privacy breaches in the health care sector make it less likely for patients to disclose sensitive information to their physicians.

It has been the WRHA's experience that being able to provide assurances to individuals that they would be notified if they or their privacy was put at risk because of the breach of the confidentiality of their PHI (e.g., snooping or a lost document) has proven helpful in building trust with the people who come to us for health care.

Notification may be not just to the individuals, it can also be to the applicable regulator (which in Manitoba is the Ombudsman). We recognize that a supervisory function performed by the Ombudsman can play a valuable role in ensuring that adequate protections of privacy are in place and are being complied with. The WRHA enjoys a good working relationship with the Office of the Ombudsman, and values the role that the Ombudsman plays in ensuring the privacy of the PHI and personal information of Manitobans. There are many occasions where notification to the Ombudsman of the occurrence of a privacy breach is appropriate. The practice of the WRHA is to notify the Ombudsman of breaches based on the same

[14] www.ponemon.org

considerations as are described here whether to notify the individuals affected. It is submitted that these considerations should equally apply.

Other jurisdictions have recognized the benefits of a reasoned breach notification requirement and have enshrined it in law. Notably, Ontario has determined that breach notification to the Information Privacy Commissioner will be mandatory. The Yukon *Health Information Privacy and Management Act* takes a more moderate approach and addresses these considerations as follows:

> 30(1) If a security breach occurs in relation to an individual's personal health information in a custodian's custody or control, and there are reasonable grounds to believe that the individual is at risk of significant harm as a result of the security breach, the custodian must, as soon as reasonably possible after the security breach, notify the individual of the security breach.

An added example may be found in the legislation of Nova Scotia who has adopted the following provisions:

> 69 Subject to the exceptions and additional requirements, if any, that are prescribed, a custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity if the custodian believes on a reasonable basis that
> (a) the information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification; and
> (b) as a result, there is potential for harm or embarrassment to the individual.
>
> 70(1) Where a custodian determines on a reasonable basis that personal health information has been stolen, lost or subject to unauthorized access, use, disclosure, copying or modification, but
> (a) it is unlikely that a breach of the personal health information has occurred; or
> (b) there is no potential for harm or embarrassment to the individual as a result, the custodian may decide that notification to the individual pursuant to section 69 is not required.

Similarly, the federal personal privacy legislation, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA) was amended by the *Digital Privacy Act* (which amendment is not yet in effect) to provide for mandatory reporting as follows:

> 10.1(1) An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

(2) The report shall contain the prescribed information and shall be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.
(3) Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.
(4) The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It shall also contain any other prescribed information.
(5) The notification shall be conspicuous and shall be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it shall be given indirectly in the prescribed form and manner.
(6) The notification shall be given as soon as feasible after the organization determines that the breach has occurred.
(7) For the purpose of this section, "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.
(8) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include
    (a) the sensitivity of the personal information involved in the breach;
    (b) the probability that the personal information has been, is being or will be misused; and
    (c) any other prescribed factor.

The concept of "real risk of significant harm", like the Yukon's "risk of significant harm", presents a valuable threshold in ensuring that a balance is achieved in protecting the privacy interests of individuals, while recognizing whether there is a material risk of harm, what risk mitigation steps have been implemented and whether they are expected to be effective, and the practical administrative burden on trustees.

Privacy breaches can range from the egregious (where the risk of significant harm is very real) to the accidental, such as a care provider accidentally clicking on the name of someone which is the same or very similar to the name of the patient being cared for, immediately realizing it and closing the file. Though all WRHA personnel are trained in PHIA and mindful of their obligations under the law and policy, minor human errors of this nature do occur. Further, minor breaches of this nature pose no discernible risk of harm to the individual and have no discernible benefit to be gained through notification. To the contrary, mandatory notifications of this nature may result in a reduction in trust of care providers as described above, and might even discourage voluntary reporting of breaches by system users if they see no benefit in doing so.

Though the WRHA is in favour of mandatory notifications where significant risk of harm exists, we caution that mandatory notification of all breaches including those that have been sufficiently mitigated would have other costs and consequences that far outweigh any perceived benefit of notification.

It is instead recommended that PHIA consider an approach that requires trustees to implement policies and procedures to determine risk to individuals for any unauthorized collection, use, disclosure or destruction of PHI, whether significant risk of harm exists and/or has not been sufficiently mitigated, and when there is reason to believe that a person's PHI has been wilfully targeted or subject to snooping, that notifying the individuals affected be required under the law. The recommended approach is in keeping with current WRHA practice.[15]

For additional consideration, the American Health Information Management Association[16] defines low-risk breaches that should be exempt from mandatory breach notification as:

> Good faith, unintentional acquisition, access, or use of PHI by a workforce member.
>
> Inadvertent disclosure to another authorized person within the entity or its business associates.
>
> Recipient could not reasonably have retained the data.
>
> Data is limited to a limited data set that does not include dates of birth or zip codes.

We recommend that PHIA adopt an approach similar to that of the above cited jurisdictions whereby trustees must report breaches associated with risk of significant harm as determined by trustee policies and supported by ministerial guideline if so required.

[15] For examples of what may be considered risk of significant harm see The Information Privacy Commissioners of Ontario Mandatory Reporting From https://www.oipc.ab.ca/media/621643/breach_Reporting_tool_2012.pdf

[16] http://csrc.nist.gov/news_events/HIPAA-May2011_workshop/presentations/day2_HIPAA-conference2011-breach-risk-harm-assessment.pdf

18. Safeguards for Sensitive Information

PHIA requires that:

> Safeguards for sensitive information
> 19 In determining the reasonableness of security safeguards required under section 18, a trustee shall take into account the degree of sensitivity of the personal health information to be protected.

As health care providers, the WRHA understands that sensitivity of PHI may be highly subjective. Accordingly, WRHA's operational standard is to avoid placing subjective interpretations of sensitivity and rather to consider likelihood of re-identification of potentially identifiable PHI as a measure for security safeguards. In other words, under this approach, all identifiable PHI is treated as strictly confidential and subject to security safeguards. Within a partially de-identified data set, level of risk, rather than sensitivity, is determined by such considerations as unique level of quasi-identifiers, sample size, k-anonymity, etc., as discussed earlier in this Report.

With electronic information systems it is difficult, if not impossible, to distinguish between different categories of PHI, whether based on an assessment of sensitivity, or otherwise.

We recommend that this Section be repealed, or be reworded to reflect that sensitivity of PHI is largely subjective. Instead, it is recommended that PHIA underscore the trustee obligation of treating any and all identifiable PHI as strictly confidential.

19. PHIA Regulation

19.1 *Orientation and Training for Employees*

The PHIA Regulation provides that:

> 6 A trustee shall provide orientation and ongoing training for its employees and agents about the trustee's policy and procedures referred to in section 2.

The WRHA has recently adopted a policy that requires that every employee and affiliate of the WRHA undergo this training at least once every three years. It has been our experience that over time the appreciation of details associated with training may lessen leaving an employee at risk of breaching their obligations. The retraining requirement aims to ensure that PHIA obligations are fresh and top of mind for all WRHA employees and affiliates. It is recommended that PHIA adopt this or a similar requirement as follows:

> A trustee shall provide orientation and ongoing training for its employees and agents about the trustee's policy and procedures referred to in section 2, and shall be repeated at minimum once every 3 years.

19.2 *Pledge of Confidentiality*

The Regulation further requires that:

> 7 A trustee shall ensure that each employee and agent signs a pledge of confidentiality that includes an acknowledgment that he or she is bound by the policy and procedures referred to in section 2 and is aware of the consequences of breaching them.

In an effort to ensure access to ongoing individual level training for all WRHA employees, the WRHA employs a variety of training options including online training through the WRHA Learning Management System (LMS). The person taking the PHIA training course on LMS expressly indicates agreement with a pledge. This is a practice common to many online agreements. The Regulation should be updated by replacing "signs" with "agrees to".

19.3 *Disclosure for Charitable Fundraising*

PHIA Subsection 23.2(2) authorizes disclosure of PHI for fundraising purposes under specific conditions, including that "the trustee and the foundation comply with any additional requirements specified in the regulations."

The Regulation provides that:

> 8.1(2) A trustee must not disclose personal health information under subsection 23.2(2) of the Act in any of the following circumstances:
> (a) the trustee is a hospital and the reason for the patient's admission would reasonably be considered to be sensitive personal health information.

As discussed previously, the process of applying a subjective lens of sensitivity to the PHI of another person is fraught with risk. The best practice is to treat all PHI as confidential. To avoid a subjective consideration of sensitivity, we recommend that Subsection 8.1(2)(a) of the Regulation be amended to read as follows:

> (a) the trustee is a hospital and the reason for the patient's admission may identify information about the health of the individual or the nature of care received.

In Conclusion

PHIA remains largely effective in protecting the privacy of Manitobans' PHI. This Report identifies areas that bear strengthening to ensure that PHIA remains effective and responsive to the realities of health care delivery and health information management moving forward. The WRHA wishes to express its appreciation for the opportunity to provide its comments and recommendations and looks forward to the next stages of the consultation process.