Office of the
Saskatchewan Information
and Privacy Commissioner

STRIKING A BALANCE

Proposals for Amendments to

The Health Information Protection Act

Ronald J. Kruzeniski, K.C.

June 2016

Table of Contents

Introduction 2

Summary of Proposals 2

A. Purpose Clause 5

B. Definitions 8

C. Data Matching 17

D. Consent 19

E. Right to Information About Disclosures Without Consent 20

F. Exercise of Right or Power by Other Persons 21

G. Retention and Destruction Policy 22

H. Researchers 25

I. Access 27

J. Abandoned Requests 29

K. Third Party 29

L. Fees 31

M. Duties of Agents and Employees 33

N. Elements of Information Manager Agreement 36

O. Continuing Duties of Trustee 39

P. Deceased Individuals 40

Q. Other Uses and Disclosures 43

R. User Logs 46

S. Notification of Privacy Breach 52

T. Privacy Impact Assessments 58

U. Request for review 59

V. Powers of the Commissioner 62

W. Additional Offences and Penalties 65

X. Review of HIPA 67

Y. Inter-jurisdictional Investigations 68

Z. Whistleblower Protection 70

Introduction

The Health Information Protection Act (HIPA) came into force September 1, 2003 but has not undergone a formal legislative review. However, there have been some amendments related to employee snooping and abandoned patient records that came into force June 1, 2016. In addition, some regulations were also added (i.e. fundraising and disclosures to police) in this time period.

These amendments are intended to strike a balance between access and privacy.

This document sets out a series of proposed amendments to HIPA that attempt to achieve a number of objectives including the following:

- Reduce timelines in certain cases so patients can access their personal health information sooner;
- Ensure that the law is in step with the ever changing digital health care environment;
- Reduce or eliminate confusion/barriers that may hamper the provision of health services;
- Increase accountability and transparency with new notification and reporting requirements;
- Further discourage snooping into patient records; and
- Clarify the authority for the use and disclosure of personal health information for some secondary purposes.

Summary of Proposals

A. Purpose Clause – There is presently no object or purpose clause in HIPA. It is proposed that a purpose clause be added.

B. Definitions – Some key definitions of HIPA are missing or need to be clarified. Those include health services, disclosure, next of kin, research, genetic information, trustee, agent or employee, and record of user activity. These changes are proposed.

C. Data Matching – HIPA does not define or set rules for data matching. Both are proposed to make it clear that authority must exist if data matching is to be undertaken by a trustee.

D. Consent – Clarification is provided for when express consent is required when using or disclosing personal health information for employment related purposes. It is also proposed that the subsection that authorizes collection for any purpose with consent is repealed as is overly broad.

E. Right to Information About Disclosures Without Consent – It is proposed replacing subsection 10(2) of HIPA as it gives trustees permission to not inform patients/individuals of disclosures permitted by subsection 27(2). Trustees should be prepared to provide details of these disclosures unless not reasonably practicable.

F. Exercise of Right or Power by Other Person – Clarification is required in terms of which Minister is responsible for *The Rehabilitation Act*. This is provided.

G. Retention and Destruction Policy – Presently, HIPA offers no direction as to how long personal health information must be retained. It is proposed that a minimum retention period is adopted by trustees and that if de-identified, information may be retained for purposes other than the original purpose for which it was collected.

H. Researchers - HIPA's section 29 provides the rules around the use and disclosure of personal health information for research purposes, but could be stronger in terms of ensuring accountability. It is proposed that researchers enter into written agreements for this purpose.

I. Access – HIPA presently does not address circumstances when access should be provided within short time limits nor does it address providing access in electronic form or through patient portals. These amendments are proposed.

J. Abandoned Requests – It is proposed that HIPA include a section that clarifies when a request can be considered abandoned.

K. Third Party – HIPA does not explicitly state that any affected third party has a right to make representations in the course of a review. It is proposed that this right is extended to affected third parties.

L. Fees – Additional clarification is provided in terms of what fees a trustee may charge and when a fee waiver may be granted.

M. Duties of Agents and Employees – It is proposed that additional sections be added to HIPA that require trustees take measures to ensure its agents and employees comply with the Act including requiring orientation and ongoing training but also the signing of oaths of confidentiality.

N. Elements of Information Manager Agreements – HIPA does not presently require trustees to enter into written agreements with information management service providers (IMSPs). This should be a mandatory requirement containing specific elements as outlined.

O. Continuing Duties of Trustees – It is proposed that HIPA include a provision that clarifies responsibilities for costs associated with a failure to carry out duties under HIPA related to section 22.

P. Deceased Individuals – Additional use and disclosure provisions are proposed to assist in the identification of individuals and processing of insurance claims, to authorize the release of information to descendants for health care related purposes and to facilitate the wishes of the individual when it comes to donation of body parts, tissue or other bodily substances.

Q. Other Uses and Disclosures – A similar provision involving the deceased's wishes with regard to donations of body parts, etc is required in the case the individual is living. Other amendments proposed including authorization for the use of personal health information for educating employees or students, for risk or error management and to disclose to the Canadian Institute for Health Information (CIHI).

R. User Logs – HIPA does not presently contain any provisions regarding user activity logs. The proposal requires trustees to create and maintain records of user activity and maintain these records for at least three years. Auditing is also required. It is also clarified that no fees may be charged to the individual when a copy is requested.

S. Notification of Privacy Breach – It is proposed that mandatory breach notification is included in HIPA.

T. Privacy Impact Assessments (PIA) - It is proposed that HIPA contain a provision that requires trustees to complete and submit PIAs to the Commissioner in certain circumstances.

U. Request for Review – HIPA is silent on the Commissioner's ability to review fees and extensions and should include additional grounds for when the Commissioner may dismiss a request for review as well as access to information requests. It is proposed that language is included to expand the Commissioner's abilities to do so.

V. Powers of the Commissioner - It is proposed that HIPA clearly states that the Commissioner has the same powers in an investigation as in a review including the right to enter premises as is explicit in FOIP and that the Commissioner has the right to set his or her own procedures including having the discretion to disclose information to any person when is necessary to protect the privacy, health or safety of an individual or when in the public interest.

W. Additional Offences and Penalties – The proposed amendments would make it clear that no personal shall knowingly collect, use, disclose, create, access or attempt to access personal health information in contravention of HIPA. It is also proposed that a specific offence be created for researchers that knowingly violate written agreements with trustees.

X. Review of HIPA - In order to ensure that HIPA is reviewed regularly, it is proposed it be amended to make the process mandatory every five years.

Y. Inter-jurisdictional Investigations - It is proposed that HIPA has a section similar to Alberta to enable information sharing with other oversight bodies when an investigation involves more than one jurisdiction.

Z. Whistleblower Protection – It is suggested that a whistleblower provision be included in HIPA along the lines of similar provisions in British Columbia especially noting that *The Public Interest Disclosure Act* does not apply to trustees.

A. Purpose Clause

Presently, HIPA does not have a purpose clause. It has a preamble. That preamble is as follows:

> WHEREAS the Legislative Assembly recognizes the following principles with respect to personal health information:
>
> THAT personal health information is private and shall be dealt with in a manner that respects the continuing interests of the individuals to whom it relates;
>
> THAT individuals provide personal health information with the expectation of confidentiality and personal privacy;
>
> THAT trustees of personal health information shall protect the confidentiality of the information and the privacy of the individuals to whom it relates;
>
> THAT the primary purpose of the collection, use and disclosure of personal health information is to benefit the individuals to whom it relates;
>
> THAT, wherever possible, the collection, use and disclosure of personal health information shall occur with the consent of the individuals to whom it relates;
>
> THAT personal health information is essential to the provision of health services;
>
> THAT, wherever possible, personal health information shall be collected directly from the individual to whom it relates;
>
> THAT personal health information shall be collected on a need-to-know basis;
>
> THAT individuals shall be able to obtain access to records of their personal health information;
>
> THAT the security, accuracy and integrity of personal health information shall be protected;
>
> THAT trustees shall be accountable to individuals with respect to the collection, use, disclosure and exercise of custody and control of personal health information;
>
> THAT trustees shall be open about policies and practices with respect to the collection, use and disclosure of personal health information;

Below are examples of purpose clauses from Alberta, Ontario, New Brunswick and Newfoundland and Labrador.

Alberta's *Health Information Act* (HIA) includes the following purpose clause:

> **Purposes of Act**
> 2 The purposes of this Act are
>
> (a) to establish strong and effective mechanisms to protect the privacy of individuals with respect to their health information and to protect the confidentiality of that information,
>
> (b) to enable health information to be shared and accessed, where appropriate, to provide health services and to manage the health system,

(c) to prescribe rules for the collection, use and disclosure of health information, which are to be carried out in the most limited manner and with the highest degree of anonymity that is possible in the circumstances,

(d) to provide individuals with a right of access to health information about themselves, subject to limited and specific exceptions as set out in this Act,

(e) to provide individuals with a right to request correction or amendment of health information about themselves,

(f) to establish strong and effective remedies for contraventions of this Act, and

(g) to provide for independent reviews of decisions made by custodians under this Act and the resolution of complaints under this Act.

Ontario's *Personal Health Information Protection Act* (PHIPA) contains the following purpose clause:

Purposes

1 The purposes of this Act are,

(a) to establish rules for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information, while facilitating the effective provision of health care;

(b) to provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions set out in this Act;

(c) to provide individuals with a right to require the correction or amendment of personal health information about themselves, subject to limited and specific exceptions set out in this Act;

(d) to provide for independent review and resolution of complaints with respect to personal health information; and

(e) to provide effective remedies for contraventions of this Act.

New Brunswick's *Personal Health Information Privacy and Access Act's* (PHIPAA) purpose clause is as follows:

Purposes

2 The purposes of this Act are

(a) to provide individuals with a right to examine and receive a copy of their personal health information maintained by a custodian, subject to the limited and specific exceptions set out in this Act,

(b) to provide individuals with the right to request the correction of or amendment to their personal health information maintained by a custodian, subject to the limited and specific exceptions set out in this Act,

(c) to establish a set of rules for custodians regarding the collection, use, disclosure, retention and secure destruction of personal health information that protects the confidentiality of personal health information and the privacy of the individual to whom the personal health information relates,

(d) to facilitate the effective provision of care and planning and management of the health care system,

(e) to establish mechanisms to ensure the accountability of persons having custody or control of personal health information and to safeguard the security and integrity of the personal health information in their custody or control,

(f) to establish mechanisms to safeguard the security and integrity of personal health information by those persons having custody or control of that information,

(g) to provide for an independent review and resolution of complaints made in respect to personal health information, and

(h) to provide effective remedies for contraventions of this Act.

Newfoundland and Labrador's *Personal Health Information Act* (PHIA) contains the following purpose clause:

Purpose

3. The purposes of this Act are

(a) to establish rules for the collection, use and disclosure of personal health information that protect the confidentiality of that information and the privacy of individuals with respect to that information;

(b) to provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions set out in this Act;

(c) to provide individuals with a right to require the correction or amendment of personal health information about themselves, subject to limited and specific exceptions set out in this Act;

(d) to establish mechanisms to ensure the accountability of persons having custody or control of personal health information and to safeguard the security and integrity of the personal health information in their custody or control;

(e) to provide for an independent review of decisions and resolution of complaints with respect to personal health information in the custody or control of custodians; and

(f) to establish measures to promote the compliance with this Act by persons having the custody or control of personal health information.

Proposal

It is proposed that the preamble of HIPA be deleted and replaced with a purpose clause as follows:

Purposes of Act

XX The purposes of this Act are

(a) to establish strong and effective mechanisms to protect the privacy of individuals with respect to their personal health information and to protect the confidentiality of that information,

(b) to establish rules for the collection, use and disclosure of personal health information, which are to be carried out in the most limited manner and with the highest degree of anonymity that is possible in the circumstances while facilitating the effective provision of health care,

(c) to establish rules for the retention and destruction of personal health information that protects the confidentiality of personal health information and the privacy of the individual to whom the personal health information relates,

(d) to provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions as set out in this Act,

(e) to provide individuals with a right to require the correction or amendment of personal health information about themselves, subject to limited and specific exceptions set out in this Act;

(f) to establish mechanisms to ensure the accountability of persons having custody or control of personal health information and to safeguard the security and integrity of the personal health information in their custody or control;

(g) to enable personal health information to be shared and accessed, where appropriate, to provide health services and to manage the health system,

(h) to provide for independent review and resolution of complaints made in respect to personal health information, and

(i) to establish strong and effective remedies for contraventions of this Act.

B. Definitions

Definitions of the following terms should be included in section 2 of HIPA or where otherwise appropriate:

1. health service;
2. disclosure;
3. next of kin;
4. research;
5. genetic information;
6. expand definition of "trustee";
7. agent or employee; and
8. record of user activity.

The first definition to be considered is "health service."

1. Health Service

HIPA references both "service" and "health service" but in most cases, it is clear that what is being referred to is a health service. Neither of these terms is defined by HIPA presently.

Alberta's HIA defines health services as follows:

> 1(1)(m) "health service" means a service that is provided to an individual for any of the following purposes:

(i) protecting, promoting or maintaining physical and mental health;

(ii) preventing illness;

(iii) diagnosing and treating illness;

(iv) rehabilitation;

(v) caring for the health needs of the ill, disabled, injured or dying,

but does not include a service excluded by the regulations;

The above is far more limited than what is offered in *The Regional Health Services Administration Regulations* here in Saskatchewan as follows:

2(2.2) For the purposes of subclause 2(1)(j)(i) of the Act, the following services are health services:

(a) alcohol, drug or substance abuse or addiction assessment, education and treatment services;

(b) chronic disease management services;

(c) community health services;

(d) convalescent care and palliative care services;

(e) counselling services;

(f) diagnostic imaging services;

(g) disability management services;

(h) disease and injury prevention services;

(i) emergency medical response services;

(j) emergency stabilization services;

(k) health assessment and screening services;

(l) health education services;

(m) health promotion services;

(n) home care services;

(o) hospital services;

(p) laboratory services;

(q) long-term care services;

(r) medical services;

(s) mental health services;

(t) nursing services;

(u) personal care services;

(v) physician services;

(w) provision of drugs, medical supplies and surgical supplies;

(x) public health services;

(y) registered nurse or nurse practitioner services;

(z) rehabilitation services;

(aa) specialty and subspecialty medical services and surgical services;

(bb) therapy services;

(cc) any other goods and services ancillary or incidental to health promotion and protection or respecting the care, treatment or transportation of sick, infirm or injured individuals.

Proposal

In order to ensure consistency in Saskatchewan statutes, it is proposed that the following definition be added to the definition section of HIPA:

XX In this Act,

…

"Service" means a "health service" as defined in *The Regional Health Services Administration Regulations* but does not include a service as described in sections 11 and 28(1)(b) of this Act.

2. Disclosure

Although HIPA contains definitions of "collection" and of "use", it does not define "disclosure."

Ontario's PHIPA defines "disclose" as follows:

Definitions

2. In this Act,

"disclose", in relation to personal health information in the custody or under the control of a health information custodian or a person, means to make the information available or to release it to another health information custodian or to another person, but does not include to use the information, and "disclosure" has a corresponding meaning;

Yukon's *Health Information Privacy and Management Act* (HIPMA) defines disclose as follows:

2(1) In this Act

…

"disclose", in relation to information in the custody or control of a person, means making the information available or releasing it to another person, but includes neither using the information nor its transmission between a custodian and an agent of that custodian;

A simple definition is offered by the Northwest Territories' *Health Information Act* (HIA) as follows:

"disclose", in relation to information, means to release information or make information available in any manner, including verbally or visually, to a person or organization;

Nova Scotia's *Personal Health Information Act* (PHIA) contains the following definition of "disclose":

> 3 In this Act,
>
> …
>
> (h) "disclose", in relation to personal health information in the custody or under the control of a custodian or a person, means to make the information available or to release it to another custodian or to another person, but does not include to use the information;

Proposal

It is proposed that Nova Scotia's definition is adopted as follows:

> (x) "disclose", in relation to personal health information in the custody or under the control of a trustee, means to make the information available or to release it to another trustee or to another person, but does not include to use the information;

3. Next of Kin

"Next of Kin" is not defined in HIPA. British Columbia, Nova Scotia, Newfoundland and Labrador and the Northwest Territories use the term "next of kin" in their privacy legislation in the same manner as section 29(2)(n) of *The Freedom of Information and Protection of Privacy Act* (FOIP) in Saskatchewan. None of these statutes however offer a further definition of next of kin.

Next of kin could generally be defined as mother, father, children, brothers, sisters, grandparents, aunts, uncles, nieces, nephews and a spouse and adult interdependent partner of a person, or any of them. Depending on the statute, "next of kin" may mean one particular individual or sometimes one of many relatives or family members.

In the event that the individual is deceased, other jurisdictions allow for disclosure to more than just immediate family or those to whom the individual has a close personal relationship. For example, Nova Scotia's PHIA includes the following language:

> **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.
>
> ...
>
> 40(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.

Proposal

It is proposed that the following definition be added to section 2:

(y) “next of kin” means mother, father, children, brothers, sisters, grandparents, aunts, uncles, nieces, nephews, grandchildren and a spouse and adult interdependent partner of a person, or any of them

4. Research

“Research” is presently not defined in HIPA. Research is defined by Newfoundland and Labrador’s PHIA as follows:

2. (1) In this Act

…

(v) "research" means a systematic investigation designed to develop or establish principles or facts or to generate knowledge, or any combination of principles, facts and knowledge, and includes the development, testing and evaluation of research;

New Brunswick’s PHIPAA contains the same language as above.

Nova Scotia’s PHIA also clarifies the following:

Research
53 Planning and management of the health system does not constitute research for the purpose of this Act.

Proposal

The inclusion of the above definition in HIPA’s section 2 is proposed.

5. Genetic Information

Genetic information could be expressly added to the definition of “personal health information” to prevent any disagreement as to whether or not it is captured.

Genetic information is part of the definition of personal health information in Newfoundland and Labrador’s PHIA as follows:

Definitions
1 The following definitions apply in this Act

…

“personal health information” means identifying information about an individual in oral or recorded form if the information

(a) relates to the individual’s physical or mental health, family history or health care history, including genetic information about the individual,

New Brunswick's PHIPAA is worded the same as Newfoundland and Labrador.

Proposal

The present HIPA definition of personal health information could be amended as follows:

> **Interpretation**
> 2 In this Act:
> …
> (m) "personal health information" means, with respect to an individual, whether living or deceased:
> (i) information with respect to the physical or mental health of the individual, **including genetic information about the individual**;

6. Trustee

The definition of trustee in subsection 2(t) does not accommodate the situation where personal health information is in the custody or control of an organization that does not otherwise qualify as a trustee. This could be a municipality or a private corporation owned by persons who are not health professionals. Professionals today have chosen various forms of organizing themselves. This includes corporations, etc. The problem is that patient files exist and it would seem completely unfair for a patient to lose the protection of HIPA just because of a different organizational structure. The issue of non-trustee owners of health facilities in subsection 2(t)(xv) needs to be addressed.

Ontario's PHIPA includes the following in its definition of custodian:

> **Health Information Custodian**
> 3(1) In this Act,
> "health information custodian", subject to subsections (3) to (11), means a person or organization described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties or the work described in the paragraph, if any:
> …
> 4. A person who operates one of the following facilities, programs or services:
> i. A hospital within the meaning of the *Public Hospitals Act*, a private hospital within the meaning of the *Private Hospitals Act*, a psychiatric facility within the meaning of the *Mental Health Act* or an independent health facility within the meaning of the *Independent Health Facilities Act*.
> ii. A long-term care home within the meaning of the *Long-Term Care Homes Act, 2007*, a placement co-ordinator described in subsection 40 (1) of that Act, or a care home within the meaning of the *Residential Tenancies Act, 2006*.
> iii. a retirement home within the meaning of the *Retirement Homes Act, 2010*.
> iv. A pharmacy within the meaning of Part VI of the *Drug and Pharmacies Regulation Act*.

v. A laboratory or a specimen collection centre as defined in section 5 of the *Laboratory and Specimen Collection Centre Licensing Act*.

vi. An ambulance service within the meaning of the *Ambulance Act*.

vii. A home for special care within the meaning of the *Homes for Special Care Act*.

viii. A centre, program or service for community health or mental health whose primary purpose is the provision of health care.

Proposal

In HIPA, most of the above organizations are already captured by the definition of trustee but the definition is useful as it introduces the language "a person who operates" and "clinic operators."

Proposed is that the following clause be added to subsection 2(t) of HIPA:

(xv) a person who operates a facility whose primary purpose is the provision of health services provided by health professionals licensed or registered pursuant to an Act.

7. Agent or Employee

HIPA does not include a definition of employee and does not explicitly capture other persons or organizations outside of information management service providers (IMSP). The Yukon in its HIPMA has the following definition of "agent":

2(1) In this Act

"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.

Ontario's PHIPA has the following simpler definition of agent:

2. In this Act,

"agent", in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the

authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated;

In *It's Time to Update: Proposals for Amendments to FOIP and LA FOIP* (*It's Time to Update*), I proposed the following definition of employee as follows:

2(k) "employee", in relation to government institution (local authority), includes a person who performs a service for the government institution (local authority) as an appointee, officer, volunteer or student or under a contract or agency relationship with the government institution (local authority);

Proposal

It is proposed that a definition of employee be defined by HIPA as follows:

2 In this Act,

…

(f) "employee", in relation to a trustee organization, includes a person who performs a service for the trustee as an appointee, officer, volunteer or students in training for the purpose of obtaining a degree, certificate or diploma or professional designation or under a contract or agency relationship with the trustee and includes an information management service provider;

8. Record of User Activity

HIPA presently does not define or contain provisions requiring trustees to maintain records of user activity. Yukon's HIPMA includes the following definition:

Definitions
2(1) In this Act
…
"record of user activity" means a record created in accordance with subsection 22(3);

Manitoba's PHIA Regulation offers the following broader definition of "record of user activity":

Definitions
1 In this regulation,
…
"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;

Nova Scotia's *Personal Health Information Regulations* requires the following with respect to record of user activity:

Record of user activity
11(1) In subsection 63(3) of the Act and in this Section, "record of user activity related to an individual's personal health information" means a report produced at the request of an individual for a list of users who accessed the individual's personal health information on an electronic information system for a time period specified by the individual.

(2) A record of user activity related to an individual's personal health information must include at least all of the following information:

(a) the name of the individual whose personal health information was accessed;

(b) a unique identification number for the individual whose personal health information was accessed, including their health-card number or a number assigned by the custodian to uniquely identify the individual;

(c) the name of the person who accessed the personal health information;

(d) any additional identification of the person who accessed the personal health information, including an electronic information system user identification name or number;

(e) a description of the personal health information accessed or, if the specific personal health information accessed cannot be determined, all possible personal health information that could have been accessed;

(f) the date and time the personal health information was accessed or, if specific dates and times cannot be determined, a range of dates when the information could have been accessed by the person.

(3) A custodian must retain the information that was used to update a record of user activity related to an individual's personal health information for at least 1 year after each date of access.

Proposal

Proposed is a definition including elements from Manitoba and Nova Scotia as follows:

(x)"record of user activity" means a record about access to personal health information maintained on an electronic information system, which identifies at least 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) a description of the personal health information accessed or, if the specific personal health information accessed cannot be determined, all possible personal health information that could have been accessed;

C. Data Matching

Data matching or data linkage becomes a concern primarily if the intention is to use personal health information for secondary purposes. HIPA presently does not contain any provisions regarding data matching or data linkage. The following provisions regarding data matching is taken from Alberta's HIA:

Interpretation
1(1) In this Act,

…

(g) "data matching" means the creation of individually identifying health information by combining individually identifying or non-identifying health information or other information from 2 or more electronic databases, without the consent of the individuals who are the subjects of the information;

Nova Scotia's *Personal Health Information Regulation* does not define data matching but does offer the following definition of "data linkage":

2 (1) In the Act,

"data linkage" means the bringing together of 2 or more records of personal health information to form a composite record;

HIPA also does not presently set out rules associated with using data for data matching purposes. New Brunswick's PHIPAA includes the following section regarding data matching:

Data matching
57(1) A custodian shall not, in contravention of this Act,

(a) collect personal health information to be used in data matching, or

(b) use or disclose personal health information to be used in data matching or created through data matching.

57(2) A custodian may perform data matching using personal health information in its custody or control, provided there is authority for the collection, use or disclosure of the personal health information being used for data matching or created as a result of data matching.

Alberta's HIA contains the following language pertaining to data matching:

Prohibition
68 A custodian or health information repository must not

(a) collect the health information to be used in data matching,

or

(b) use or disclose the health information to be used in data matching or created through data matching in contravention of this Act.

Data matching by custodian or health information repository
69 A custodian or health information repository may perform data matching using information that is in its custody or under its control.

Data matching by custodians or health information repository
70(1) A custodian or health information repository may perform data matching by combining information that is in its custody or under its control with information that is in the custody or under the control of another custodian or health information repository.

(2) Before performing data matching under this section, the custodian or health information repository in whose custody and control the information that is created through data matching will be stored must prepare a privacy impact assessment and submit the assessment to the Commissioner for review and comment.

(3) A privacy impact assessment referred to in subsection (2) must

(a) describe how the information to be used in the data matching is to be collected, and

(b) set out how the information that is created through data matching is to be used or disclosed.

Data matching by custodian or health information repository and non-custodian
71(1) A custodian or health information repository may perform data matching by combining information that is in its custody or under its control with information that is in the custody or under the control of a person that is not a custodian or health information repository.

(2) Before performing data matching under this section, the custodian or health information repository must prepare a privacy impact assessment and submit the assessment to the Commissioner for review and comment.

(3) A privacy impact assessment referred to in subsection (2) must meet the requirements of section 70(3).

Data matching for research
72 If data matching is performed for the purpose of conducting research, sections 48 to 56 must be complied with before the data matching is performed.

Proposal

Proposed is that a similar definition from Alberta be added to HIPA in section 2 as follows:

(x) “data matching” means the creation of individually identifying personal health information by combining individually identifying or non‑identifying health information or other information from 2 or more electronic databases;

Also proposed is to include the following sections in HIPA pertaining to data matching:

Data matching
X(1) Subject to subsections (2), (3), and (4) a trustee shall not,

(a) collect personal health information to be used in data matching, or

(b) use or disclose personal health information to be used in data matching or created through data matching.

XX(2) A trustee may perform data matching using personal health information in its custody or control, provided there is authority for the collection, use or disclosure of the personal health information being used for data matching or created as a result of data matching.

XX(3) A trustee may use personal health information in data matching if the data matching is for a secondary purpose consistent with any of the purposes for which personal health information may be disclosed pursuant to section 27, 28 or 29.

XX(4) Nothing in this section prohibits the data matching of personal health information where that data matching is authorized by another Act or by a regulation made pursuant to another Act.

D. Consent

Additional clarification is proposed for HIPA when it comes to consent requirements and considerations.

1. Express Consent Required for Employment Purposes

It should be made clear in subsection 26(3) of HIPA that express consent is required for the purpose of accessing or using personal health information for employment related purposes as are distinctively different than providing diagnosis, treatment or care where consent may be implied. For instance, Ontario's PHIPA, personal health information does not include employee information used for purposes other than health care as follows:

Exception
4 (4) Personal health information does not include identifying information contained in a record that is in the custody or under the control of a health information custodian if,

(a) the identifying information contained in the record relates primarily to one or more employees or other agents of the custodian; and

(b) the record is maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employees or other agents.

Proposal

It is proposed that HIPA be amended as follows:

26(3) Nothing in subsection (2) authorizes a trustee as an employer to use or obtain access to the personal health information of an individual who is an employee or prospective employee for any purpose related to the employment of the individual without the individual's **express** consent.

2. Consent Provision Without Limits

Presently, subsection 24(4) of HIPA reads as follows:

> 24(4) A trustee may collect personal health information for any purpose with the consent of the subject individual.

The above wording opens up the potential for abuse as it does not explicitly require "express" consent of the patient, and could authorize the collection of personal health information for purposes completely unrelated to diagnosis, treatment or care and other many secondary purposes already authorized.

Proposal

It is proposed that subsection 24(4) of HIPA be repealed.

E. Right to Information About Disclosures Without Consent

Section 10 of HIPA requires a trustee to take reasonable steps to ensure that it is able to inform an individual about any disclosures of that individual's personal information made without the individual's consent. It does not however, require a record of those disclosures to be maintained.

Nova Scotia's PHIA requires such records to be kept as follows:

> 42 (1) A disclosure of health information without consent must be documented.
>
> (2) The documentation must include
>
> (a) a description or copy of the personal health information disclosed;
>
> (b) the name of the person or organization to whom the personal health information was disclosed;
>
> (c) the date of the disclosure; and
>
> (d) the authority for the disclosure.

Newfoundland and Labrador's PHIA also requires documentation of disclosures as follows:

> **Maintaining certain disclosure information**
> 48.(1) Except as otherwise provided under subsection (2) or section 37, a custodian that discloses personal health information shall make a note of the following:
>
> (a) the name of the person to whom the custodian discloses the information;
>
> (b) the date and purpose of the disclosure; and
>
> (c) a description of the information disclosed.
>
> (2) Subsection (1) does not apply where a custodian discloses personal health information by permitting access to the information stored in the information system of the custodian, provided

that when the information is accessed, the database automatically keeps an electronic log of the following information:

(a) the user identification of the person that accesses the information;

(b) the date and time the information is accessed; and

(c) a description of the information that is accessed or that could have been accessed.

The Northwest Territory's HIA also requires a record of disclosure as follows:

84. (1) Subject to subsections (2) and (3), a health information custodian that discloses personal health information about an individual without his or her express consent, shall make a record of

(a) the name of the person or organization to which the information is disclosed;

(b) the date of the disclosure;

(c) the purpose of the disclosure; and

(d) a description of the information disclosed.

…

(3) Subsection (1) does not apply where a health information custodian discloses personal health information by permitting collection of information from an electronic record stored in an electronic health information system, if the system automatically keeps an electronic log

(a) of the user identification of the person who collects the information;

(b) of the date and time the information is collected; and

(c) that identifies the information that is collected or that could have been collected.

Proposal

It is proposed that subsection 10(2) of HIPA is amended as it gives trustees permission to not inform patients/individuals of disclosures permitted by subsection 27(2). Subsection 10(2) should be replaced with the following wording.

10(2) A disclosure of personal health information without consent must be documented unless the information system accessed automatically keeps a record of user activity or is not reasonably practicable.

F. Exercise of Right or Power by Other Persons

Subsection 56(e)(i) of HIPA states:

(e) where the individual does not have the capacity to give consent:

(i) by a person designated by the Minister of Community Resources and Employment if the individual is receiving services pursuant to *The Residential Services Act* or *The Rehabilitation Act*;

Proposal

It is proposed that the provision now refer to the Ministry of Social Services.

G. Retention and Destruction Policy

Subsection 17(1) of HIPA related to retention and destruction of personal health information is "not yet proclaimed" and provides as follows:

> 17 (1) A trustee must:
>
> (a) have a written policy concerning the retention and destruction of personal health information that meets the requirements set out in the regulations; and
>
> (b) comply with that policy and any prescribed standards with respect to the retention and destruction of personal health information.

A very important part of the protection of patient data is knowing that at some point the data is destroyed. Once it is destroyed it cannot be accidently released or abandoned.

Currently, *The Hospital Standards Regulations 1980* contains retention guidelines for personal health information. Section 15(1) reads as:

> 15(1) Subject to subsection (2), the patient's health record shall be retained by the hospital for a minimum period of ten years from the date of last discharge or until age 19 if the patient is a minor, whichever period is longer or for such further period as may be deemed necessary by the hospital after consultation with the medical staff.
>
> (2) Where microfilming is employed, the health record must be retained in its original form for a minimum period of 6 complete years, and the microfilm must be retained for the remainder of the retention period mentioned in subsection (1).

The College of Physicians and Surgeons for the province of Saskatchewan has regulatory bylaws. Section 23.1 (f) reads as follows:

> A member shall retain the records required by this regulation for six years after the date of the last entry in the record. Records of pediatric patients shall be retained until 2 years past the age of majority or 6 years after the date last seen, whichever may be the later date.

Nova Scotia's PHIA contains the following in its section on retention, destruction, disposal and de-identification:

> 47 Sections 48 to 51 apply to personal health information in both paper records and an electronic information system.
>
> 48 A custodian shall have in place and comply with information practices that meet the requirements of this Act.

49 (1) In this Section, "securely destroyed" means destroyed in such a manner that reconstruction is not reasonably foreseeable in the circumstances.

(2) At the expiry of the relevant retention period, personal health information that is no longer required to fulfil the purposes identified in the retention schedule must be securely destroyed, erased or de-identified.

(3) Subject to Section 50, personal health information may be de-identified and retained for purposes other than the original purposes for which it was collected.

…

50 (1) Every custodian shall have a written retention schedule for personal health information that includes

(a) all legitimate purposes for retaining the information; and

(b) the retention period and destruction schedules associated with each purpose.

(2) Subsection (1) does not override or modify any requirement in an enactment of the Province or the Parliament of Canada concerning the retention or destruction of records maintained by public bodies.

New Brunswick's PHIPAA includes the following language:

Requirements for retention, storage and secure destruction of information
55(1) A custodian shall establish and comply with a written policy for the retention, archival storage, access and secure destruction of personal health information that

(a) meets any requirements prescribed by regulation or any requirements contained in any Act of the Legislature,

(b) protects the privacy of the individual to whom the information relates, and

(c) requires that a custodian who destroys personal health information to keep a record of the individual whose personal health information is destroyed, a summary of the contents of the record, the time period to which the information relates, the method of destruction and the name of the person responsible for supervising the secure destruction.

55(2) Unless otherwise provided in the regulations, a public body shall ensure that personal health information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:

(a) if the individual to whom the information relates has identified the information and has consented, in the manner prescribed by regulation, to it being stored in another jurisdiction;

(b) if the information is stored in another jurisdiction for the purpose of disclosure allowed under this Act;

(c) if the information was disclosed for the purposes of:

(i) a payment to be made to or by the Province or a public body,

(ii) authorizing, administering, processing, verifying or cancelling a payment to be made to or by the Province or a public body, or

(iii) resolving an issue regarding a payment to be made to or by the Province of or a public body.

55(3) This section does not override or modify any requirement in an Act of the Legislature or the Parliament of Canada concerning the retention or secure destruction of records maintained by a public body.

Manitoba's PHIA contains the following language:

Retention and destruction policy
17(1) A trustee shall establish a written policy concerning the retention and destruction of personal health information and shall comply with that policy.

Compliance with regulations
17(2) A policy under subsection (1) must conform with any requirements of the regulations.

Method of destruction must protect privacy
17(3) In accordance with any requirements of the regulations, a trustee shall ensure that personal health information is destroyed in a manner that protects the privacy of the individual the information is about.

17(4) [Repealed] S.M. 2008, c. 41, s. 9.

Application of this section
17(5) This section does not override or modify any requirement in an enactment of Manitoba or Canada concerning the retention or destruction of records maintained by public bodies.

Nova Scotia's PHIA includes a section for written retention schedules as follows:

Written retention schedule
50 (1) Every custodian shall have a written retention schedule for personal health information that includes:

(a) all legitimate purposes for retaining the information;

and

(b) the retention period and destruction schedules associated with each purpose.

(2) Subsection (1) does not override or modify any requirement in an enactment of the Province or the Parliament of Canada concerning the retention or destruction of records maintained by public bodies.

Proposal

It is proposed that subsection 17(1) of HIPA be replaced with the following:

Retention and destruction policy
17(1) Every trustee must have a written retention schedule for personal health information that includes a minimum period of ten years from the date of last discharge or until age 19 or if the patient is a minor, whichever is longer.

17(1.1) Subject to subsection (1), personal health information may be de-identified and retained for purposes other than the original purposes for which it was collected.

Subsection 17(1.1) may not be necessary as subsection 3(2) of HIPA indicates that HIPA does not apply to de-identified information. Subsection 17(1.1) is proposed nonetheless to provide greater certainty.

H. Researchers

HIPA contains few provisions to provide guidance to trustees when dealing with researchers. HIPA's section 29 provides the rules around the use and disclosure of personal health information for research purposes, but could be stronger in terms of ensuring accountability. Alberta's HIA contains the following language that I believe could be incorporated into our existing provision:

54(1) If the custodian decides to disclose health information to a researcher, the researcher must enter into an agreement with the custodian in which the researcher agrees:

(a) to comply with

(i) this Act and the regulations made under this Act,

(ii) any conditions imposed by the custodian relating to the use, protection, disclosure, return or disposal of the health information, and

(iii) any requirement imposed by the custodian to provide safeguards against the identification, direct or indirect, of an individual who is the subject of the health information,

(b) to use the health information only for the purpose of conducting the proposed research,

(c) not to publish the health information in a form that could reasonably enable the identity of an individual who is the subject of the information to be readily ascertained,

(d) not to make any attempt to contact an individual who is the subject of the health information to obtain additional health information unless the individual has provided the custodian with the consent referred to in section 55,

(e) to allow the custodian to access or inspect the researcher's premises to confirm that the researcher is complying with the enactments, conditions and requirements referred to in clause (a), and

(f) to pay the costs referred to in subsection (3).

(2) When an agreement referred to in subsection (1) has been entered into, the custodian may disclose to the researcher the health information requested under section 52

(a) with the consent of the individuals who are the subjects of the information, where the ethics committee recommends that consents should be obtained, or

(b) without the consent of the individuals who are the subjects of the information, where the ethics committee does not recommend that consents be obtained.

(3) The custodian may set the costs of

(a) preparing information for disclosure,

(b) making copies of health information, and

(c) obtaining the consents referred to in section 55,

which must not exceed the actual cost of providing that service.

(4) If the researcher contravenes or fails to meet the terms and conditions of an agreement under this section, the agreement is cancelled.

Subsection 29(3) of *The Archives and Public Records Management Act* clarifies obligations of researchers as follows:

29(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:

...

(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.

Proposal

It is proposed that subsection 29(1)(c) and (d) of HIPA be amended to read as follows:

29(1)(c) before disclosing the personal health information to the researcher, the researcher enters into a written agreement with the trustee or designated archive:

(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 trustee or designated archive 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 trustee or designated archive 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.

(d) If the researcher contravenes or fails to meet the terms and conditions of an agreement under this section, the agreement is cancelled.

Also proposed is that the same language above replace 29(2)(b) and (d) of HIPA as well so both subsections require researchers to enter into written agreements before being provided access to personal health information.

I. Access

Waiting for up to 30 days for access to personal health information may be too long for some patients to wait.

1. Timely Access

There are times that waiting up to 30 days for access to one's patient record is unreasonable. Manitoba's PHIA sets out a time limit of 24 hours within which a trustee shall respond to a request by a hospital in-patient to examine his or her personal health information provides as follows:

Trustee to respond promptly

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;

Information provided in 24 hours

6(1.1) In the circumstance mentioned in clause (1)(a) (hospital patient), the trustee is required only to make the information available for examination and may or may not, despite section 7, provide a copy.

Failure to respond

6(3) The failure of a trustee to respond to a request within the time frame required under subsection (1) is to be treated as a decision to refuse to permit the personal health information to be examined or copied.

Proposal

It is proposed that Saskatchewan's HIPA should contain similar language as the above in Part V, Access of Individuals to Personal Health Information, specifically the following:

> 33(2) A trustee with a facility that is a hospital shall respond to an oral request as promptly as required in the circumstances but not later than 24 hours after receiving it if the information is about health care currently being provided to an in-patient.
>
> (3) In the circumstance mentioned in 33(2) (hospital patient), the trustee is required only to make the information available for examination and may or may not provide a copy.

2. Unconventional Access

a. Electronic Form

The right of access under HIPA is to "personal health information about himself or herself that is contained in a record in the custody or control of a trustee." In terms of providing access, subsection 36 requires that the trustee make the personal health information "available for examination" and "providing a copy, if requested, to the applicant." However, it may be cheaper, faster and more convenient for patients to receive the information electronically. BC's FOIP contains a provision that we may want to adopt as follows:

> 9(2.1) If the applicant has asked for a copy under section 5 (2) in electronic form and it is reasonable to provide the record in that form, a copy of the record or part of the record must be provided in that form with the response.

Proposal

It is proposed that the above wording be added to section 36 of HIPA as follows:

> **36**(1) Within 30 days after receiving a written request for access, a trustee must respond to the request in one of the following ways:
>
> (a) by making the personal health information available for examination and providing a copy, if requested, to the applicant; or
>
> **(i) if the applicant has asked for a copy under section 34 in electronic form and it is reasonable to provide the record in that form, a copy of the record or part of the record must be provided in that form with the response;**

b. Patient Portals

HIPA does not have a provision to specifically authorize the use of patient portals for providing access to patient records. eHealth Saskatchewan is piloting the Citizen Health Information Portal which is a secure patient portal. Though it has more to do with fees, below is a section from Northwest Territories' *Health Information Regulation* in reference to patient portals:

> 9(3) There is no fee for the following:
>
> (a) access of personal health information through a patient portal;

Proposal

It is proposed that HIPA contain a similar provision to Northwest Territories' Regulation as follows:

> 39(5) There is no fee for access of personal health information through a patient portal;

J. Abandoned Requests

HIPA does not clarify when an access request may be considered abandoned. This office proposed a similar amendment in FOIP. Alberta's HIA has the following wording regarding abandoned requests:

> 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.
>
> (2) A notice declaring a request abandoned must state that the applicant may ask for a review of that decision by the Commissioner.

Proposal

It is proposed that HIPA is amended to include a similar provision to that found in Alberta as follows:

> XX (1) Where the trustee or its agent 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 trustee or its agent as requested, within 30 days after being contacted, the trustee or its agent may, by notice in writing to the applicant, declare the request abandoned.
>
> (2) A notice under subsection (1) must state that the applicant may ask for a review by the commissioner.

The above is the same language that this office proposed in our *It's Time to Update* publication.

K. Third Party

Currently HIPA in Part VI does not allow for third party intervention. Presently, HIPA's section 45 provides as follows:

> **Conduct of review**
> 45(1) The commissioner shall conduct a review in private.

(2) The applicant and the trustee whose decision is the subject of a review are entitled to make representations to the commissioner in the course of the review.

(3) No one is entitled as of right:

(a) to be present during a review; or

(b) before or after a review, to have access to, or to comment on, representations made to the commissioner by any other person.

Alberta's HIA provides for circumstances when others may intervene as follows:

Notifying others of review
75(1) On receiving a request for a review, the Commissioner must as soon as practicable

(a) give a copy of the request

(i) to the custodian concerned, and

(ii) to any other person who in the opinion of the Commissioner is affected by the request,

and

(b) provide a summary of the review procedures and an anticipated date for a decision in respect of the review

(i) to the person who asked for the review,

(ii) to the custodian concerned, and

(iii) to any other person who in the opinion of the Commissioner is affected by the request.

(2) Despite subsection (1)(a), the Commissioner may sever any information in the request that the Commissioner considers appropriate before giving a copy of the request to the custodian or any other person affected by the request.

Proposal

It is proposed that language similar to that found in Alberta above be added to section 45 of HIPA as follows:

Conduct of review
45(1) The commissioner shall conduct a review in private.

(2) The applicant, the trustee whose decision is the subject of a review **and any other person, who in the opinion of the Commissioner is affected by the review**, are entitled to make representations to the commissioner in the course of the review.

L. Fees

HIPA only contains one provision that speaks to fees which provides as follows:

> 39 A trustee may charge a reasonable fee not exceeding the prescribed amount to recover costs incurred in providing access to a record containing personal health information.

1. Fee Schedule

HIPA should have a fee schedule**.**

Alberta's HIA contains the following language:

> **Power to charge fees**
> 67(1) A custodian may charge the fees provided for in the regulations for services provided under Part 2.
>
> (2) Subsection (1) does not permit a custodian to charge a fee in respect of a request for access to an applicant's own health information, except for the cost of producing the copy.
>
> (3) A custodian must give an applicant an estimate of the total fee for its services before providing the services.

New Brunswick's Regulation under PHIPAA includes the following provisions regarding fees:

> **Search and preparation fees**
> 9(1) An individual shall pay a search and preparation fee to a custodian if the custodian estimates that search and preparation related to the individual's request to examine or receive a copy of the individual's personal health information takes more than 2 hours.
>
> 9(2) The fee payable for search and preparation shall be $15 for each half-hour beyond the first 2 hours of search and preparation related to the individual's request.
>
> **Copying fees**
> 10 An individual shall pay the following copying fees to the custodian when the individual makes a request to examine or receive a copy of the individual's personal health information:
>
> (a) if the information in relation to the request is stored or recorded in printed form and able to be copied using a photocopier or computer printer, 25 cents for each page copied;
>
> (b) if the information in relation to the request is not able to be copied using a photocopier or computer printer, the actual cost of providing copies of the request.

Nova Scotia's PHIA does not allow a custodian to charge for a record of user activity as follows:

> 63(4) A custodian shall not charge an individual for a record of user activity.

Proposal

The following new language is proposed for section 39 of HIPA:

> 39(1) A trustee shall not charge a fee, except for the cost of producing the record, for access to an applicant's own personal health information if the search and preparation time is less than 2 hours.
>
> (2) An individual shall pay a search and preparation fee to a trustee if the trustee estimates that search and preparation related to the individual's request to examine or receive a copy of the individual's personal health information takes more than 2 hours, not to exceed fees as prescribed in the regulations.
>
> (3) Where time in excess of two hours is spent in searching for a record requested by the applicant or in preparing it for disclosure, the trustee must give an applicant an estimate of the total fee for its services before providing the services of an amount no greater than $400.
>
> (4) Where the amount of an estimate exceeds the actual amount of fees determined pursuant to (2), the actual amount of fees is the amount payable by the applicant.

2. Waiver of Fees

Section 39 of HIPA does not include a fee waiver provision.

Alberta's HIA contains the following language:

> 67(4) A custodian may excuse an applicant from paying all or part of a fee if, in the opinion of the custodian, the applicant cannot afford the fee or in any other circumstances provided for in the regulations.
>
> (5) If an applicant has requested a custodian to excuse the applicant from paying all or part of a fee and the custodian has refused the applicant's request, the custodian must notify the applicant that the applicant may ask for a review by the Commissioner.

Nova Scotia's PHIA includes the following fee waiver provision:

> **Fees**
> 82 (3) A custodian has the discretion to determine whether to grant a fee waiver and may waive the payment of all or any part of the fee that an individual is required to pay under that subsection if, in the custodian's opinion, the individual cannot afford the payment or for any other reason it is fair to excuse payment.

Alberta's *Health Information Regulation* includes the following fee waiver provision:

> 13 For the purposes of section 67(4) of the Act, a custodian may excuse an applicant from paying all or part of a fee if in the opinion of the custodian it is fair to excuse payment.

The comparable provision in Ontario's PHIPA is:

> 54(12) A health information custodian mentioned in subsection (10) may waive the payment of all or any part of the fee that an individual is required to pay under that subsection if, in the custodian's opinion, it is fair and equitable to do so.

Saskatchewan's FOIP Regulations fee waiver provision provides as follows:

> **Waiver of fees**
> 9 For the purposes of subsection 9(5) of the Act, the following circumstances are prescribed as circumstances in which a head may waive payment of fees:
>
> (a) where the actual cost of responding to an application varies from the total of the prescribed fees that are applicable to the application;
>
> (b) where payment of the prescribed fees will cause a substantial financial hardship for the applicant and:
>
> (i) in the opinion of the head, giving access to the record is in the public interest; or
>
> (ii) the application involves the personal information of the applicant;
>
> (c) where the prescribed fee or actual cost for the service is $10 or less.

Proposal

It is proposed that the following amendment is made to section 39 of HIPA modelled on Nova Scotia as follows:

> 39(6) If an individual requests a fee waiver, a trustee has the discretion to determine whether to grant a fee waiver and may waive the payment of all or any part of the fee that an individual is required to pay under that subsection if, in the trustee's opinion, the individual cannot afford the payment or for any other reason it is fair to excuse payment.

M. Duties of Agents and Employees

HIPA could provide more in terms of the duties of employees and others. Yukon's HIPMA lays out the responsibilities and duties of agents as follows:

> **Responsibilities of custodians and agents**
> 49 A custodian must take reasonable measures to ensure that its agents comply with this Act and the regulations.
>
> **Duties of agent**
> 50(1) A custodian may permit its agent to collect, use, disclose, retain, destroy or dispose of personal health information on the custodian's behalf only if
>
> (a) the custodian is permitted or required to collect, use, disclose, retain, destroy or dispose of the information, as the case may be;
>
> (b) the collection, use, disclosure, retention, destruction or disposition of the information, as the case may be, is in the course of the agent's duties and is not contrary to the limits imposed by the custodian, this Act or any other enactment;
>
> (c) the custodian allows the agent to use only that personal health information that the agent needs in order to carry out the purpose for which it was collected or a purpose for which use is authorized under this Act; and

(d) the prescribed requirements, if any, are met.

(2) Except as permitted or required by law, an agent of a custodian must not collect, use, disclose, retain, destroy or dispose of personal health information on the custodian's behalf unless the custodian permits the agent to do so in accordance with subsection (1).

(3) An agent of a custodian must notify the custodian at the first reasonable opportunity if a security breach has occurred in relation to any personal health information handled by the agent.

Newfoundland and Labrador's PHIA sets out clear obligations of employee, etc. by requiring the following:

Obligations of employees, etc.
14. (1) A custodian shall ensure that

(a) its employees, agents, contractors and volunteers; and

(b) where the custodian is an operator of a health care facility, those health care professionals who have the right to treat persons at a health care facility operated by the custodian,

take an oath or affirmation of confidentiality.

(2) A custodian's employees, agents, contractors and volunteers, and those health care professionals who have the right to treat persons at a health care facility operated by the custodian shall comply with

(a) this Act and the regulations; and

(b) the information policies and procedures referred to in subsection 13(1).

(3) A custodian shall ensure that its employees, agents, contractors and volunteers, and those health care professionals who have the right to treat persons at a health care facility operated by the custodian are aware of the duties imposed by this Act and the regulations and the information policies and procedures referred to in section 13.

(4) A person who provides goods or services for the purpose of enabling a custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with this Act and the regulations.

HIPA speaks to a trustee's responsibility to have policies and procedures but does not explicitly require training in those policies and procedures. Manitoba's PHIA Regulation has a specific provision on orientation and training of employees as follows:

Orientation and training for employees
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.

In addition, HIPA's sections 16 and 23 could be modified to include some of the following from Newfoundland and Labrador's PHIA as is broader in application:

Information practices, policies and procedures
13. (1) A custodian that has custody or control of personal health information shall establish and implement information policies and procedures to facilitate the implementation of, and ensure compliance with, this Act and the regulations respecting the manner of collection, storage, transfer, copying, modification, use and disposition of personal information whether within or outside the province.

(2) The information policies and procedures referred to in subsection (1) shall include policies and procedures to

(a) protect the confidentiality of personal health information that is in its custody or under its control and the privacy of the individual who is the subject of that information;

(b) restrict access to an individual's personal health information by an employee, agent, contractor or volunteer of the custodian or by a health care professional who has the right to treat persons at a health care facility operated by the custodian to only that information that the employee, agent, contractor, volunteer or health care professional requires to carry out the purpose for which the information was collected or will be used;

(c) protect the confidentiality of personal health information that will be stored or used in a jurisdiction outside the province or that is to be disclosed by the custodian to a person in another jurisdiction and the privacy of the individual who is the subject of that information; and

(d) provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information.

(3) The information policies and procedures referred to in subsection (1) shall include appropriate measures to address the risks associated with the storage of personal health information, taking into account the manner and form in which the personal health information is recorded, the location of storage and the degree of sensitivity of the personal health information to be protected.

Proposal

It is proposed that clauses 16(c) be expanded and (d) be introduced to HIPA as follows:

Duty to protect
16 Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:

…

(c) otherwise ensure compliance with this Act by its employees by including that

(i) its employees, agents, contractors and volunteers take an oath or affirmation of confidentiality;

(d) The information policies and procedures referred to in subsection (1) shall include appropriate measures to address the risks associated with the storage of personal health information, taking into account the manner and form in which the personal health information is recorded, the location of storage and the degree of sensitivity of the personal health information to be protected.

Further, it is proposed that (2.1) below be added to section 23:

> **Collection, use and disclosure on need-to-know basis**
> 23(1) A trustee shall collect, use or disclose only the personal health information that is reasonably necessary for the purpose for which it is being collected, used or disclosed.
>
> (2) A trustee must establish policies and procedures to restrict access by the trustee's employees to an individual's personal health information that is not required by the employee to carry out the purpose for which the information was collected or to carry out a purpose authorized pursuant to this Act.
>
> **(2.1) A trustee shall provide orientation and ongoing training for its employees and agents about the trustee's policy and procedures referred to in subsection (2).**
>
> (3) Repealed. 2003, c.25, s.13.
>
> (4) A trustee must, where practicable, use or disclose only de-identified personal health information if it will serve the purpose.

N. Elements of Information Manager Agreement

Presently subsections 18(2) and (4) of HIPA have not been proclaimed into force. Those subsections read as follows:

> 18(2) Before providing personal health information to an information management service provider, a trustee must enter into a written agreement with the information management service provider that:
>
> (a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the information;
>
> (b) provides for protection of the information; and
>
> (c) meets the requirements of the regulations.
>
> ...
>
> (4) An information management service provider must comply with the terms of the agreement entered into pursuant to subsection (2).

If a trustee has an arrangement with an information manager or IMSP, it seems only reasonable that that arrangement only be in a written contract. It would allow for assurances of confidentiality by employees, guarantee the type of data protection and solidify agreement on when the records would be destroyed. Many government institutions require a contract from other institutions when institutions need access to data. It seems very fair and reasonable to require trustees to request a contract. In fact, such a contract is for both the protection of the trustee and the IMSP. HIPA contains provisions for IMSPs in section 18 but does not provide explicit language for what should be included in the agreements. I have proposed in *It's Time to Update,* the following amendments for FOIP and LA FOIP:

> XX (1) A government institution (local authority) may provide personal information to an information management service provider or consultant:

(a) for the purpose of having the information management service provider process, store, archive or destroy the personal information for the government institution (local authority);

(b) to enable the information management service provider to provide the government institution (local authority) with information management or information technology services;

(c) for the purpose of having the information management service provider take custody and control of the personal information;

(d) for the purpose of combining records containing personal information; or

(e) for the purpose of providing consulting services.

(2) Before providing personal information to an information management service provider, contractor or consultant, a government institution (local authority) must enter into a written agreement with the information management service provider, contractor or consultant that:

(a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the information;

(b) provides for protection of the information; and

(c) meets the requirements of the Act and regulations.

(3) An information management service provider, contractor or consultant shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal information received from a government institution (local authority) except for the purposes set out in subsection (1).

(4) An information management service provider, contractor or consultant must comply with the terms of the agreement entered into pursuant to subsection (2).

Alberta's *Health Information Regulation* information manager agreement provides as follows:

Information manager agreement
7.2 For the purposes of section 66(2) of the Act, an agreement between a custodian and an information manager must

(a) identify the objectives of the agreement and the principles to guide the agreement,

(b) indicate whether or not the information manager is permitted to collect health information from any other custodian or from a person and, if so, describe that health information and the purpose for which it may be collected,

(c) indicate whether or not the information manager may use health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be used,

(d) indicate whether or not the information manager may disclose health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be disclosed,

(e) describe the process for the information manager to respond to access requests under Part 2 of the Act or, if the information manager is not to respond to access requests, describe the process for referring access requests for health information to the custodian itself,

(f) describe the process for the information manager to respond to requests to amend or correct health information under Part 2 of the Act or, if the information manager is not to respond to requests to

amend or correct health information, describe the process for referring access requests to amend or correct health information to the custodian itself,

(g) describe how health information provided to the information manager is to be protected, managed, returned or destroyed in accordance with the Act,

(h) describe how the information manager is to address an expressed wish of an individual relating to the disclosure of that individual's health information or, if the information manager is not to address an expressed wish of an individual relating to the disclosure of that individual's health information, describe the process for referring these requests to the custodian itself, and

(i) set out how an agreement can be terminated.

Yukon's HIPMA includes the following requirements:

Responsibilities of custodians and information managers
51(1) A custodian who proposes to retain the services of an information manager must

(a) enter into a written agreement with the information manager that provides for the protection of the information that is the subject of the services; and

(b) comply with the prescribed requirements, if any.

(2) An information manager who enters into a written agreement under subsection (1) must

(a) comply with the duties imposed on the information manager under the agreement and the prescribed requirements, if any; and

(b) notify the custodian at the first reasonable opportunity of any breach of the agreement by the information manager.

Proposal

The following amendment is proposed:

18(2) Before providing personal health information to an information management service provider, contractor or consultant, a trustee must enter into a written agreement with the information management service provider, contractor or consultant that:

(a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the personal health information;

(b) provides for protection of the personal health information; and

(c) meets the requirements of the Act and regulations.

(3) An information management service provider, contractor or consultant shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection (1).

(4) An information management service provider, agent, contractor or consultant must comply with the terms of the agreement entered into pursuant to subsection (2).

...

(6) An information management service provider, contractor or consultant must comply with the terms of the agreement entered into pursuant to subsection (2) and **notify the trustee at the first reasonable opportunity of any breach of the agreement**.

O. Continuing Duties of Trustee

HIPA already contains a section on continuing duties of a trustee but is lacking certain elements.

Newfoundland and Labrador's PHIA requires notice to be provided to patients when transferring patient records to a successor as follows:

> 39(2) For the purpose of paragraph (1)(j), a custodian who transfers a record of personal health information to its successor shall make reasonable efforts to give notice to the individual who is the subject of the information prior to the transfer or, where this is not possible, as soon as possible after the transfer that it has ceased to be a custodian of the information and identifying its successor.
>
> (3) Where a notice provided by a custodian under subsection (2) is in the form of a public notice, the information contained in the notice shall be limited to the following:
>
> (a) that the custodian has ceased or will cease to be a custodian within the jurisdiction;
>
> (b) the identity and contact information of its successor; and
>
> (c) the means by which an individual whose personal health information is in the custody or control of the custodian may access his or her record of personal health information after the transfer.

Yukon's HIPMA is very unique as includes a provision to spell out who is responsible for costs associated with a failure to follow the rules:

> **Continuing duties of custodian**
> 23(1) The duties imposed under this Act on a custodian with respect to personal health information, and records containing personal health information, in the custody or control of the custodian apply to the custodian until the custodian transfers custody and control of the personal health information or the records to a successor of the custodian in accordance with section 60 or to a prescribed person in accordance with the prescribed requirements, if any.
> …
>
> (4) The Minister may require a custodian who fails to carry out their duties under this Act
>
> (a) to reimburse the Government of Yukon for any costs it reasonably incurs as a result of the custodian's failure; and
>
> (b) to pay a person appointed under subsection (2) to carry out the custodian's duties an amount determined by the Minister, as compensation for the person's services under that subsection, and to reimburse the person for any disbursements it reasonably makes in providing the services.

Proposal

It is proposed that language similar to that from Newfoundland and Labrador above be added to subsection 22 of HIPA as follows:

> 22(2.1) The Minister may require a trustee who fails to carry out their duties under this section:
>
> (a) to reimburse the Government of Saskatchewan for any costs it reasonably incurs as a result of the trustee's failure; and
>
> (b) to pay a person appointed under subsection (2) to carry out the trustee's duties an amount determined by the Minister, as compensation for the person's services under that subsection, and to reimburse the person for any disbursements it reasonably makes in providing the services.

P. Deceased Individuals

Presently, HIPA authorizes limited disclosure when the data subject is deceased. In practice, the present list is insufficient and HIPA does not require the deceased wishes to be taken into consideration when making disclosure decisions.

Alberta's HIA includes the following disclosure provisions:

> 35(1) A custodian may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information
> …
>
> (d) where an individual is injured, ill or deceased, so that family members of the individual or another person with whom the individual is believed to have a close personal relationship or a friend of the individual can be contacted, if the disclosure is not contrary to the express request of the individual,
>
> (d.1) where an individual is deceased, to family members of the individual or to another person with whom the individual is believed to have had a close personal relationship, if the information relates to circumstances surrounding the death of the individual or to health services recently received by the individual and the disclosure is not contrary to the express request of the individual,
> …
>
> (o) to a descendant of a deceased individual, a person referred to in section 104(1)(c) to (i) who is acting on behalf of the descendant or a person who is providing health services to the descendant if, in the custodian's opinion,
>
> (i) the disclosure is necessary to provide health services to the descendant, and
>
> (ii) the disclosure is restricted sufficiently to protect the privacy of the deceased individual,

Newfoundland and Labrador's PHIA provides as follows:

> **Where individual deceased**
> 38. A custodian may disclose personal health information about an individual who is deceased or presumed to be deceased without the consent of the individual who is the subject of the information
>
> (a) for the purpose of identifying the individual;
>
> (b) for the purpose of informing a person whom it is reasonable to inform in the circumstances of the fact that the individual is deceased or presumed to be deceased and the circumstances of the death, where appropriate;
>
> (c) to the personal representative of the deceased for a purpose related to the administration of the estate;
>
> (d) to a spouse, partner, sibling or descendant of the individual where the recipient of the information reasonably requires the information to make decisions about his or her own health care or the health care of his or her child or where the disclosure is necessary to provide health care to the recipient; or
>
> (e) for research purposes under the authority of section 44.

The Yukon's HIPMA expands the list of authorized disclosures in a number of cases including when necessary to make insurance claims, determining wishes in relation to the donation of bodily parts and informing individuals that the individual is deceased as follows:

> **When individual is deceased**
> 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.
>
> **Use not requiring consent**
> 56(1) A custodian may, without an individual's consent, use the individual's personal health information that is in its custody or control
>
> …
>
> (e) for the purpose of determining or carrying out the individual's wishes in relation to the donation of the individual's body parts, tissue, or bodily substances;
>
> (f) if the individual is deceased, or the custodian reasonably believes the individual is deceased
>
> (i) for the purpose of identifying the deceased; or
>
> (ii) for the purpose of informing any person whom it is reasonable to inform of the fact that the individual is deceased or believed to be deceased;

Disclosures not requiring consent
58 A custodian may disclose an individual's personal health information without the individual's consent

…

(d) where the individual is deceased, or the custodian reasonably believes the individual is deceased, to an individual (referred to in this paragraph as the "proposed recipient") who is a member of the deceased's immediate family or whom the custodian reasonably believes has a close personal relationship with the deceased

(i) for the purpose of identifying the deceased,

(ii) if the custodian reasonably believes that the proposed recipient requires the personal health information to make decisions about their own health or health care, or

(iii) if the personal health information relates to circumstances surrounding the death of the deceased or to health care recently received by the deceased and the disclosure is not contrary to the express instruction of the deceased;

Presently, subsection 27(2)(c) of HIPA takes into consideration a living person's express wishes, but the same cannot be said for disclosures under subsection 27(4)(e). This provision reads as follows:

27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

…

(e) if the subject individual is deceased:

(i) where the disclosure is being made to the personal representative of the subject individual for a purpose related to the administration of the subject individual's estate; or

(ii) where the information relates to circumstances surrounding the death of the subject individual or services recently received by the subject individual, and the disclosure:

(A) is made to a member of the subject individual's immediate family or to anyone else with whom the subject individual had a close personal relationship; and

(B) is made in accordance with established policies and procedures of the trustee, or where the trustee is a health professional, made in accordance with the ethical practices of that profession;

Proposal

It is proposed that the following sub-clauses be added to subsection 27(4)(e) of HIPA:

27(4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

…

(e) if the subject individual is deceased:

(i) where the disclosure is being made to the personal representative of the subject individual for a purpose related to the administration of the subject individual's estate; or

(ii) to the Coroner, law enforcement, funeral directors, next of kin or anyone else prescribed for the purpose of identifying the individual;

(iii) to a next of kin of the individual where the recipient of the information reasonably requires the information to make decisions about his or her own health care or the health care of his or her child or where the disclosure is necessary to provide health care to the recipient;

(iv) where it relates to a claim under a policy of insurance in which a benefit is payable upon the death of the deceased;

(v) for the purpose of informing any person whom it is reasonable to inform of the fact that the individual is deceased or believed to be deceased;

(vi) for the purpose of determining or carrying out the individual's wishes in relation to the donation of the individual's body parts, tissue, or bodily substances;

(vi) where the information relates to circumstances surrounding the death of the subject individual or services recently received by the subject individual, and the disclosure:

(A) is made to a member of the subject individual's immediate family or to anyone else with whom the subject individual had a close personal relationship; and

(B) is made in accordance with established policies and procedures of the trustee, or where the trustee is a health professional, made in accordance with the ethical practices of that profession;

It is also proposed that the language below be added to subsection 27(4)(e)(ii):

(C) the subject individual has not expressed a contrary intention to a disclosure of that type.

Q. Other Uses and Disclosures

HIPA is not clear in terms of when it is appropriate to use or disclose personal health information for certain secondary purposes.

Some other secondary purposes are legitimate needs of the system but not presently clearly authorized by HIPA are explored in this section. These include risk and error management, quality improvement, education, internal management and sharing with family members in certain circumstances. However, de-identified information should be relied on wherever possible.

Newfoundland and Labrador's PHIA includes the following:

Permitted uses
34. A custodian may use personal health information its custody or under its control for one or more of the following purposes:
…

(d) for the purpose of risk management or error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of related programs or services of the custodian;

Ontario's PHIPA provides as follows:

Permitted use

37. (1) A health information custodian may use personal health information about an individual,

…

(d) for the purpose of risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the custodian;

(e) for educating agents to provide health care;

Alberta HIA authorizes use without consent for the following secondary purposes:

Use of individually identifying health information

27(1) A custodian may use individually identifying health information in its custody or under its control for the following purposes:

…

(c) conducting investigations, discipline proceedings, practice reviews or inspections relating to the members of a health profession or health discipline;

…

(e) providing for health services provider education;

…

(g) for internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.

From the Yukon's HIPMA is the following:

Use not requiring consent

56(1) A custodian may, without an individual's consent, use the individual's personal health information that is in its custody or control

…

(i) for the purpose of payment, or for contractual or other legal requirements, in respect of the custodian's provision to the individual of health care or other related goods, services or benefits, including goods, services or benefits that are part of a program of the custodian;

…

(l) for the purpose of managing or auditing the health care activities of the custodian;

Disclosures not requiring consent

58 A custodian may disclose an individual's personal health information without the individual's consent

…

(f) for the purpose of determining or carrying out the individual's wishes in relation to the donation of the individual's body parts, tissue, or bodily substances;

…

(n) to the Canadian Institute for Health Information, or to a prescribed health data institute in Canada that has entered into a written agreement with the Minister governing its collection, use and disclosure of the personal health information;

…

(dd) to a person conducting an audit, reviewing an application for accreditation or conducting an accreditation, if the audit, review or accreditation relates to the services provided by the custodian and the person has agreed in writing before commencing the audit, review or accreditation process

(i) to destroy the personal health information at the earliest possible opportunity after completing the audit, review or accreditation, and

(ii) not to disclose the personal health information to any other person, except as required to accomplish the audit, review or accreditation or to report unlawful conduct by the custodian; or

Proposal

It is proposed that an additional subsection be added to section 26, which might provide as follows:

26(2) A trustee may provide authorization for the use of personal health information about an individual

...

(d) for educating its employees to provide health services, if it is not reasonably practicable for the consent of the subject individual to be obtained;

The inclusion of the following provisions to subsection 27(4) of HIPA is further proposed:

27 (4) A trustee may disclose personal health information in the custody or control of the trustee without the consent of the subject individual in the following cases:

...

(q) for the purpose of determining or carrying out the individual's wishes in relation to the donation of the individual's body parts, tissue, or bodily substances;

(r) to a person conducting an audit, reviewing an application for accreditation or conducting an accreditation, if the audit, review or accreditation relates to the services provided by the trustee and the person has agreed in writing before commencing the audit, review or accreditation process;

(i) to destroy the personal health information at the earliest possible opportunity after completing the audit, review or accreditation, and

(ii) not to disclose the personal health information to any other person, except as required to accomplish the audit, review or accreditation or as required by law; or

(s) to the Canadian Institute for Health Information after entering into a written agreement; or

(t) for the purpose of risk management, error management or for the purpose of activities to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of the trustee.

R. User Logs

An aspect of a role-based access electronic model is the need to monitor it by auditing uses and disclosures of personal health information of users of the system. Auditing should be mandated in legislation. Proactive audits should also be required on a regular basis.

It is important that individuals have the ability to find out who has accessed their records. With electronic health records this means that individuals must have the right to see the audit logs that contain information about who has accessed their record and when.

Presently, for example, a patient is able to request an audit report of who has looked at his or her eHR Viewer record. All views of personal health information are tracked including the name of the health care provider who viewed the information, the time and date that the information was viewed and what was looked at. It is not legally required by HIPA at this point but should be.

From Alberta's HIA is the following on this topic:

> **Maintaining record of Alberta EHR information**
> 56.6(1) If an authorized custodian uses prescribed health information pursuant to section 56.5, the authorized custodian must keep an electronic log of the following information:
>
> (a) a name or number that identifies the custodian who uses the information;
>
> (b) the date and time that the information is used;
>
> (c) a description of the information that is used.
>
> (2) The information referred to in subsection (1) must be retained by the authorized custodian for a period of 10 years following the date of the use.
>
> (3) An individual who is the subject of information referred to in subsection (1) may ask the authorized custodian or the information manager of the Alberta EHR for access to and a copy of the information, and Part 2 applies to the request.
>
> (4) If, pursuant to subsection (3), an individual asks the information manager of the Alberta EHR for access to and a copy of the information referred to in subsection (1), the information manager of the Alberta EHR must, in accordance with Part 2, provide that information in respect of all custodians who have used that individual's prescribed health information pursuant to section 56.5.

Alberta's *Electronic Health Record Regulation* contains the following on logging:

Logging capacity required

6(1) A custodian must ensure its electronic health record information system creates and maintains logs containing the following information:

(a) user identification and application identification associated with an access;

(b) name of user and application that performs an access;

(c) role or job functions of user who performs an access;

(d) date of an access;

(e) time of an access;

(f) actions performed by a user during an access, including, without limitation, creating, viewing, editing and deleting information;

(g) name of facility or organization at which an access is performed;

(h) display screen number or reference;

(i) personal health number of the individual in respect of whom an access is performed;

(j) name of the individual in respect of whom an access is performed;

(k) any other information required by the Minister.

(2) This section applies only to electronic health record information systems established after the coming into force of this section.

Audit of information logs

7 The information manager of the Alberta EHR shall conduct an audit each month of the information logs of the Alberta EHR.

From Yukon's HIPMA is the following on recording requirements:

Recording requirements

22(1) If a custodian discloses any of an individual's personal health information to a person without the individual's consent, the custodian must record

…

(3) A custodian must create and maintain, or cause to be created and maintained, for any electronic information system the custodian uses to maintain personal health information, a record of user activity that includes, in respect of each incident of access by a person, through the system, to personal health information or personal information

(a) the person's user identification;

(b) the date and time of the incident;

(c) a description of the information that is accessed or that could have been accessed; and

(d) any prescribed information.

(4) A record of user activity under subsection (3) must meet the prescribed requirements, if any.

The following is already available through eHealth Saskatchewan, to a certain extent, so should be formalized. This would also address the need to deal with other electronic legacy systems. The following is also from the Yukon:

> **Right of access**
> 24(3) If a custodian uses electronic means to collect, use or disclose an individual's personal health information
>
> (a) the right of access includes, subject to any prescribed limitations, the right to obtain a copy of a record of user activity of the individual's personal health information; and
>
> (b) despite subsection (2), the custodian must not charge a fee for providing such a copy.
>
> …
>
> **Record of user activity**
> 76 Any person who operates an electronic information system designated under paragraph 72(2)(a) shall maintain a record of user activity that identifies every instance in which YHIN information is accessed through the designated system.

Newfoundland and Labrador's PHIA provides as follows:

> **Maintaining certain disclosure information**
> 48. (1) Except as otherwise provided under subsection (2) or section 37, a custodian that discloses personal health information shall make a note of the following:
>
> (a) the name of the person to whom the custodian discloses the information;
>
> (b) the date and purpose of the disclosure; and
>
> (c) a description of the information disclosed.
>
> (2) Subsection (1) does not apply where a custodian discloses personal health information by permitting access to the information stored in the information system of the custodian, provided that when the information is accessed, the database automatically keeps an electronic log of the following information:
>
> (a) the user identification of the person that accesses the information;
>
> (b) the date and time the information is accessed; and
>
> (c) a description of the information that is accessed or that could have been accessed.

Manitoba's PHIA's Regulation offers the following:

> **Additional safeguards for electronic health information systems**
> 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(2) A record of user activity may be generated manually or electronically.
>
> 4(3) In the following circumstances, a record of user activity is not required under this section:

(a) if personal health information is demographic or eligibility information listed in Schedule B, or is information that qualifies or further describes information listed in Schedule B;

(b) if personal health information is disclosed under the authority of clause 22(2)(h) of the Act (disclosure to a computerized health information network) in a routine and documented transmission from one electronic information system to another;

(c) if personal health information is accessed or disclosed while a trustee is generating, distributing or receiving a statistical report, as long as the trustee

(i) maintains a record of the persons authorized to generate, distribute and receive such reports, and

(ii) regularly reviews the authorizations.

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.

The following is taken from Ontario Bill 78, *Electronic Personal Health Information Protection Act, 2014*:

Functions and responsibilities re electronic health record
55.3 (1) A prescribed organization shall exercise the following functions with respect to the electronic health record:

1. Carrying out its responsibilities under Part V and this Part.

2. Any other functions prescribed in the regulations.

Requirements re electronic health record
(2) A prescribed organization shall comply with the following requirements in creating or maintaining the electronic health record:

1. It shall take reasonable steps to limit the personal health information it receives to that which is reasonably necessary for the purpose of creating or maintaining the electronic health record.

2. It shall not permit its employees or any other person acting on its behalf to view, handle or otherwise deal with the personal health information received for the purpose of creating or maintaining the electronic health record, unless the employee or person acting on behalf of the prescribed organization agrees to comply with the restrictions that apply to the prescribed organization.

3. It shall make available to the public and to each health information custodian that provided personal health information to it for the purpose of creating or maintaining the electronic health record,

i. a plain language description of the electronic health record, including a general description of the administrative, technical and physical safeguards in place to,

A. protect against theft, loss and unauthorized collection, use or disclosure of personal health information in the electronic health record,

B. protect the electronic health record against unauthorized copying, modification or disposal, and

C. protect the integrity, security and confidentiality of the personal health information in the electronic health record, and

ii. any directives, guidelines and policies of the prescribed organization that apply to the personal health information in the electronic health record to the extent that these do not reveal a trade secret or confidential scientific, technical, commercial or labour relations information.

4. It shall,

i. keep an electronic record of all instances where all or part of the personal health information in the electronic health record is viewed, handled or otherwise dealt with, and shall ensure that the record identifies the individual to whom the information relates, the type of information that is viewed, handled or otherwise dealt with, all persons who have viewed, handled or otherwise dealt with the information, and the date, time and location of the viewing, handling, or dealing with, and

ii. in the event that a health information custodian has requested that the prescribed organization transfer to the custodian personal health information in the electronic health record, keep an electronic record of all instances where all or part of the personal health information in the electronic health record is transferred to the custodian, and ensure that the record identifies the individual to whom the information relates, the type of information that is transferred, the custodian requesting the information, the date and time that the information was transferred, and the location to which the information was transferred.

5. It shall keep an electronic record of all instances where a consent directive is made, withdrawn or modified, and shall ensure that the record identifies the individual who made, withdrew or modified the consent directive, the instructions that the individual provided regarding the consent directive, the health information custodian, agent or other person to whom the directive is made, withdrawn or modified, and the date and time that the consent directive was made, withdrawn or modified.

6. It shall keep an electronic record of all instances where all or part of the personal health information in the electronic health record is disclosed under section 55.6 and shall ensure that the record identifies the health information custodian that disclosed the information, the health information custodian who collected the information, any agent who collected the information on a custodian's behalf, the individual to whom the information relates, the type of information that was disclosed, the date and time of the disclosure and the purpose of the disclosure.

7. It shall audit and monitor the electronic records that it is required to keep under paragraphs 4, 5 and 6.

8. It shall, upon the request of the Commissioner provide to the Commissioner, for the purposes of Part VI, the electronic records kept under paragraphs 4, 5 and 6.

9. It shall, upon request of a health information custodian who requires the records to audit and monitor its compliance with this Act, provide to the custodian or an agent acting on the custodian's behalf, the records kept under paragraphs 4, 5 and 6.

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.

11. It shall notify, at the first reasonable opportunity, a health information custodian that provided it with personal health information for the purpose of creating or maintaining the electronic health record if the personal health information that the health information custodian provided is stolen, lost or accessed by unauthorized persons.

12. It shall,

i. make available to each health information custodian that provided personal health information to the prescribed organization for the purpose of creating or maintaining the electronic health record a written copy of the results of the assessment carried out under paragraph 10 that relates to the personal health information the custodian provided, and

ii. make available to the public a summary of the results of the assessments carried out under paragraph 10.

13. It shall ensure that any third party it retains to assist in providing services for the purpose of creating or maintaining the electronic health record agrees to comply with the restrictions and conditions that are necessary to enable the prescribed organization to comply with all these requirements.

14. It shall have in place and comply with practices and procedures,

i. that are for the purpose of protecting the privacy of the individuals whose personal health information it receives for the purpose of creating or maintaining the electronic health record and for maintaining the confidentiality of the information, and

ii. that are approved by the Commissioner every three years.

15. It shall notify the Commissioner, in writing, immediately after becoming aware that personal health information in the electronic health record,

i. has been viewed, handled or otherwise dealt with by the prescribed organization or a third party retained by the prescribed organization, other than in accordance with this Act or its regulations, or

ii. has been made available or released by the prescribed organization or a third party retained by the prescribed organization, other than in accordance with this Act or its regulations.

16. It shall submit to the Commissioner, at least annually, a report in the form and manner specified by the Commissioner, and based on or containing any information, other than personal health information, that is kept in the electronic record required under paragraph 6 that the Commissioner may specify, respecting every instance in which personal health information was disclosed under section 55.6 since the time of the last report.

17. It shall comply with the practices and procedures prescribed in the regulations when managing consent directives.

18. It shall have in place and comply with practices and procedures that have been approved by the Minister for responding to or facilitating a response to a request made by an individual under Part V in respect of the individual's records of personal health information in the electronic health record created or maintained by the prescribed organization.

19. It shall comply with such other requirements as may be prescribed in the regulations.

Proposal

The following amendment is proposed:

Additional safeguards for electronic health information systems
XX(1) A trustee shall create and maintain a record of user activity for any electronic information system it uses to maintain personal health information unless not reasonably practicable.

(2) A trustee shall audit records of user activity to detect privacy or security breaches, as prescribed in the regulations.

(3) A trustee shall maintain a record of user activity for at least three years.

Also, proposed is the addition of subsection (2) to section 32 that would ensure that individuals have a right to access records of user activities as follows:

32(2) If a trustee uses electronic means to collect, use or disclose an individual's personal health information

(a) the right of access includes, subject to any prescribed limitations, the right to obtain a copy of a record of user activity of the individual's personal health information including the name of the person who accessed the personal health information; and

(b) the trustee shall not charge a fee for providing such a copy.

S. Notification of Privacy Breach

On June 10, 2015, the Ontario Government announced that it would make it mandatory to report privacy breaches to the Information and Privacy Commissioner and, in certain cases, to relevant regulatory colleges. Saskatchewan should follow suit. There should also be a legislative requirement to provide breach notification to affected individuals in certain circumstances.

It has also been recommended in a BC IPC special report (https://www.oipc.bc.ca/special-reports/1634) that the Commissioner's office be advised of privacy breaches on a consistent basis so it can monitor and provide advice on such issues as the appropriate notice that should be given to individuals. Further, given the amount and nature of personal health information that could be disclosed in a privacy breach involving EHRs, notice to individual should be required by law as well.

For example, Alberta's *Personal Information Protection Act* (PIPA) provides as follows:

Notification of loss or unauthorized access or disclosure
34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

(2) A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.

Report to commissioner
31(1) If section 30 requires a custodian to notify an individual of a security breach in relation to the individual's personal health information in the custodian's custody or control, the custodian must, within a reasonable time after discovering the security breach, submit to the commissioner a written report that

(a) assesses the risk of harm to individuals as a result of the security breach, and estimates the number of individuals so affected; and

(b) describes the measures, if any, that the custodian has taken to reduce the risk of harm to individuals as a result of the security breach.

(2) The commissioner may, after reviewing a report submitted by a custodian under subsection (1) in respect of a security breach, recommend to the custodian any measures that the commissioner considers appropriate to reduce the risk of similar breaches occurring in the future.

In terms of defining "significant harm" and factors for determining whether a "real risk of significant harm" exists, I note the following from PIPEDA (noted as "amendments not in force"):

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 following example is taken from Yukon's HIPMA:

Notification of individual

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.

(2) Where subsection (1) requires a custodian to notify an individual of a security breach

(a) the custodian must, in the notice

(i) describe the circumstances of the security breach and the personal health information involved,

(ii) indicate when the security breach occurred,

(iii) describe the measures, if any, that the custodian has taken to reduce the risk of harm to the individual as a result of the security breach, and

(iv) identify the custodian's contact individual; and

(b) the custodian must at the same time give the commissioner a copy of the notice.

(3) In determining whether a custodian has reasonable grounds to believe that an individual is at risk of significant harm as a result of a security breach in relation to the individual's personal health information, the following are to be considered

(a) the length of time between the occurrence of the security breach and its discovery by the custodian;

(b) the likelihood that there has been any disclosure, unauthorized use or copying of the personal health information;

(c) the information available to the custodian regarding the individual's personal circumstances;

(d) the likelihood that the personal health information could be used for the purpose of identity theft or identity fraud;

(e) the number of other individuals whose personal health information is or may be similarly affected;

(f) the measures, if any, that the custodian took after the security breach to reduce the risk of harm to the individual as a result of the security breach; and

(g) any factor that is reasonably relevant in the circumstances or is prescribed for this purpose.

In Ontario's Bill 119, *An Act to amend the Personal Health Information Protection Act, 2004*, to make certain related amendments and to repeal and replace the Quality of Care Information Protection Act, 2004 (Bill 119), the following provision regarding notification is proposed:

Notice of theft, loss, etc. to individual
(2) Subject to subsection (4) and to the exceptions and additional requirements, if any, that are prescribed, if personal health information about an individual that is in the custody or control of a health information custodian is stolen or lost or if it is used or disclosed without authority, the health information custodian shall,

(a) notify the individual at the first reasonable opportunity of the theft or loss or of the unauthorized use or disclosure; and

(b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under Part VI.

Bill 119 also requires notification to be provided to regulatory bodies in the following circumstances:

17.1 (1) In this section,

"College" means,

(a) in the case of a member of health profession regulated under the *Regulated Health Professions Act, 1991*, a College of the health profession named in Schedule 1 to that Act, and

(b) in the case of a member of the Ontario College of Social Workers and Social Service Workers, that College.

Termination, suspension, etc. of employed members
(2) Subject to any exceptions and additional requirements, if any, that are prescribed, if a health information custodian employs a health care practitioner who is a member of a College, the health information custodian shall give written notice of any of the following events to the College within 30 days of the event occurring:

1. The employee is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee.

2. The employee resigns and the health information custodian has reasonable grounds to believe that the resignation is related to an investigation or other action by the custodian with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee.

Member's privileges revoked, etc.
(3) Subject to any exceptions and additional requirements, if any, that are prescribed, if a health information custodian extends privileges to, or is otherwise affiliated with, a health care practitioner who is a member of a College, the custodian shall give written notice of any of the following events to the College within 30 days of the event occurring:

1. The member's privileges are revoked, suspended or restricted, or his or her affiliation is revoked, suspended or restricted, as a result of the unauthorized collection, use, disclosure, retention or disposal of personal health information by the member.

2. The member relinquishes or voluntarily restricts his or her privileges or his or her affiliation and the health information custodian has reasonable grounds to believe that the relinquishment or restriction is related to an investigation or other action by the custodian with respect to an alleged un-authorized collection, use, disclosure, retention or disposal of personal health information by the member.

Contents of notice
(4) A notice made under this section shall meet the prescribed requirements, if any.

In *It's Time to Update*, this office proposed the following:

XX(1) For the purposes of this section, unauthorized access means a government institution (local authority) having personal information in its possession or under its control shall, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized use or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized use or disclosure.

(2) A notice to the Commissioner under subsection (1) shall include the information prescribed by the regulations.

Proposal

The following provisions similar to that of the Yukon should be added to HIPA:

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

(2) Where subsection (1) requires a trustee to notify an individual of a privacy breach

(a) the trustee must, in the notice

(i) describe the circumstances of the privacy breach and the personal health information involved,

(ii) indicate when the privacy breach occurred,

(iii) describe the measures, if any, that the trustee has taken to reduce the risk of harm to the individual as a result of the privacy breach, and

(iv) identify the trustee's contact individual; and

(b) the trustee must at the same time give the commissioner a copy of the notice.

(3) In determining whether a trustee has reasonable grounds to believe that an individual is at real risk of significant harm as a result of a privacy breach in relation to the individual's personal health information, the following are to be considered

(a) the length of time between the occurrence of the privacy breach and its discovery by the trustee;

(b) the likelihood that there has been any disclosure, unauthorized use or copying of the personal health information;

(c) the information available to the trustee regarding the individual's personal circumstances;

(d) the likelihood that the personal health information could be used for the purpose of identity theft or identity fraud;

(e) the number of other individuals whose personal health information is or may be similarly affected;

(f) the measures, if any, that the trustee took after the privacy breach to reduce the risk of harm to the individual as a result of the privacy breach; and

(g) any factor that is reasonably relevant in the circumstances or is prescribed in the regulations.

Notification to the Commissioner

XX If section XX requires a trustee to notify an individual of a privacy breach in relation to the individual's personal health information in the trustee's custody or control, the trustee must, within a reasonable time after discovering the privacy breach, submit to the commissioner a written report that

(a) assesses the risk of harm to individuals as a result of the privacy breach, and estimates the number of individuals so affected; and

(b) describes the measures, if any, that the trustee has taken to reduce the risk of harm to individuals as a result of the privacy breach.

It is also proposed that an additional section be added to HIPA for providing notice to regulatory bodies as follows:

Notice of termination, suspension, etc. of employed members

XX(1) Subject to any exceptions and additional requirements, if any, that are prescribed, if a trustee employs a health professional licensed or registered pursuant to an Act, the trustee shall give written notice of any of the following events to the health professional body that regulates that member within 30 days of the event occurring:

(a) The employee is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee.

(b) The employee resigns and the trustee has reasonable grounds to believe that the resignation is related to an investigation or other action by the trustee with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee.

T. Privacy Impact Assessments

The following quote is taken from *Operational Review of the Personal Health Information Protection and Access Act*, Department of Health, January 2015:

> Section 69 of British Columbia's *Freedom of Information and Protection of Privacy Act* requires PIAs to be conducted and established policies in that province ensure they occur for any new legislation, information system or policy. Alberta's *Health Information Act* is more inclusive. Section 64(1) of that Act states that "each custodian must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information." PIA requirements in New Brunswick are broader still, but are specific to public bodies or custodians prescribed by regulation. Under PHIPAA, public bodies must conduct PIAs when any new or modified means of collecting, using or disclosing personal health information, is being considered.

The same British Columbia Information and Privacy Commissioner special report noted earlier proposes the following: "It should be mandatory for PIAs regarding proposed administrative practices and information systems and data-linking initiatives in the health sector to be submitted to the Commissioner for review and comment. There is such a requirement in Alberta's HIA. PIAs must be submitted to the Information and Privacy Commissioner of Alberta for review and comment."

Alberta's HIA provides as follows:

> **Duty to prepare privacy impact assessment**
> 64(1) Each custodian must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information.
>
> (2) The custodian must submit the privacy impact assessment to the Commissioner for review and comment before implementing any proposed new practice or system described in subsection (1) or any proposed change to existing practices and systems described in subsection (1).

Similarly, the NWT's HIA includes the following provision regarding privacy impact assessments:

> 89. (1) In this section, "prescribed custodian" means a health information custodian prescribed as a custodian to which this section applies.
>
> (2) A public custodian and a prescribed custodian shall prepare a privacy impact assessment in respect of a proposed new, or a proposed change to an information system or communication technology relating to the collection, use or disclosure of personal health information.
>
> (3) A health information custodian to which this section applies shall give a copy of the privacy impact assessment to the Information and Privacy Commissioner.

The proposed amendments to FOIP in *It's Time to Update* are as follows:

XX(1) A government institution (local authority) must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying personal information may affect the privacy of the individual who is the subject of the information.

(2) The government institution (local authority) must submit the privacy impact assessment to the Commissioner for review and comment before implementing any proposed new practice or system described in subsection (1) or any proposed change to existing practices and systems described in subsection (1).

Proposal

Proposed is to add wording to HIPA similar to that used in *It's Time to Update* as follows:

XX(1) A trustee must prepare a privacy impact assessment that describes how any proposed substantive changes to administrative practices and information systems relating to the collection, use and disclosure of individually identifying personal health information may affect the privacy of the individual who is the subject of the information.

(2) The trustee must submit the privacy impact assessment to the Commissioner for review and comment before implementing any proposed new practice or system described in subsection (1) or any proposed change to existing practices and systems described in subsection (1).

U. Request for Review

HIPA is silent on the Commissioner's ability to take certain actions including reviewing fees and extensions and should provide for an ability to dismiss access requests or requests for review in certain circumstances.

1. Reviewing Fees and Extensions

In terms of abilities to resolve complaints, it should be explicit that the Commissioner can review fees and time extensions. The following is from Alberta's HIA:

Power to resolve complaints
85 Without limiting section 84, the Commissioner may investigate and attempt to resolve a complaint that

…

(b) an extension of time for responding to a request is not in accordance with section 15,

(c) a fee charged under this Act is inappropriate,

Under FOIP presently there is not a similar clause as above regarding fees. However, the following provision exists in FOIP regarding requesting a disagreement regarding a time extension (section 12):

Application for review
49(1) Where:

(a) an applicant is not satisfied with the decision of a head pursuant to section 7, 12 or 37;

Proposal

It is proposed that the following subsections be added to section 42 of HIPA:

42(1) A person may apply to the commissioner for a review of the matter where:

...

(d) the person is not satisfied with the decision of a trustee pursuant to section 37;

(e) the person believes that a fee charged under this Act is inappropriate.

2. Dismiss Request for Review

In *It's Time to Update*, this office proposed that section 50 in FOIP (section 39 LA FOIP) be amended to include the additional grounds referred to in HIPA, Ontario's legislation PHIPA and in the federal PIPEDA. I have taken those amendments into consideration and added a few clauses from there below.

Proposal

It is proposed that HIPA's existing subsection 43(2) be expanded as follows:

Review or refusal to review

43(2) The commissioner may refuse to conduct a review or may discontinue a review if, in the opinion of the commissioner, the application for review:

...

(e) the applicant has failed to respond to the requests of the commissioner;

(f) the trustee has responded adequately to the complaint;

(g) there is insufficient evidence to pursue the review or investigation;

(h) the matter has already been the subject of a report by the commissioner;

(i) the complaint was filed more than 2 years after the day on which the subject matter of the complaint arose;

3. Dismiss Request at Access Stage

Just as this office would propose additional language for when it is appropriate to dismiss reviews, I am proposing an amendment that would authorize dismissing requests at the application phase.

Alberta's HIA states the following:

Power to authorize a custodian to disregard requests

87(1) At the request of a custodian, the Commissioner may authorize the custodian to disregard one or more requests under section 8(1) or 13(1) if

(a) because of their repetitious or systematic nature, the requests would unreasonably interfere with the operations of the custodian or amount to an abuse of the right to make those requests, or

(b) one or more of the requests are frivolous or vexatious.

(2) The processing of a request under section 8(1) or 13(1) ceases when a custodian has made a request under subsection (1) and

(a) if the Commissioner authorizes the custodian to disregard the request, does not resume;

(b) if the Commissioner does not authorize the custodian to disregard the request, does not resume until the Commissioner advises the custodian of the Commissioner's decision.

It was proposed in *It's Time to Update*, that Saskatchewan introduces a provision in FOIP and LA FOIP similar to that used in Alberta.

XX(1) If the head of a government institution (local authority) asks, the Commissioner may authorize the government institution (local authority) to disregard one or more requests under section 7 if:

(a) 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 of access to make those requests, or

(b) one or more of the requests are frivolous or vexatious.

(2) The processing of a request under section 7 ceases when the head of a government institution (local authority) has made a request under subsection (1) and:

(a) if the Commissioner authorizes the head of the government institution (local authority) to disregard the request, it does not resume;

(b) if the Commissioner does not authorize the head of the government institution (local authority) to disregard the request, it does not resume until the Commissioner advises the head of the government institution (local authority) of the Commissioner's decision.

Proposal

The provision in HIPA similar to the above might provide as follows:

XX(1) If the trustee asks, the Commissioner may authorize the trustee to disregard one or more requests under section 36 if:

(a) 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 of access to make those requests, or

(b) one or more of the requests are frivolous or vexatious.

(2) The processing of a request under section 36 ceases when the trustee has made a request under subsection (1) and:

(a) if the Commissioner authorizes the trustee to disregard the request, it does not resume;

(b) if the Commissioner does not authorize the trustee to disregard the request, it does not resume until the Commissioner advises the trustee of the Commissioner's decision.

V. Powers of the Commissioner

Over the years, there have been times when this office has encountered trustees that are unclear as to our authority to conduct investigations including collecting necessary information, and attend at premises and interview witnesses.

1. Investigations & Production Timelines

The powers of the Commissioner in section 46 of HIPA are limited to a review. These need to be clarified so can be similarly applied when undertaking an investigation.

Further, in *It's Time to Update*, I proposed that section 54 of FOIP (section 43 LA FOIP) be amended to require the head to provide the Commissioner with the requested documents within 20 days. Wording might be as follows:

> 54(1) Notwithstanding any other Act or any privilege that is available at law, the commissioner may, in a review:
>
> (a) require to be produced and examine within 20 days, any record that is in the possession or under the control of a government institution; and

Newfoundland and Labrador's PHIA requires production however within 14 days as follows:

> 69 (3) Except as otherwise provided under subsection (4), a custodian shall produce to the commissioner a copy of the information demanded under paragraph (1)(a) within 14 days of receipt of the demand, notwithstanding another Act or regulations or a privilege under the law of evidence.

Northwest Territories' HIA also requires production in 14 days:

> 153. (1) Notwithstanding any other Act or any privilege available at law, and subject to the regulations, the Information and Privacy Commissioner may, in conducting a review under this Act, require the production of and examine any record that may be relevant to a review under this Act, that is in the custody or under the control of the health information custodian concerned.
>
> (2) Notwithstanding any other Act or any privilege available at law, and subject to subsection (3) and the regulations, a health information custodian shall produce copies of the required records for examination by the Information and Privacy Commissioner within 14 days after receiving a request for production.

Proposal

Section 46 of HIPA should be amended as bolded and underlined below:

> **Powers of commissioner**
> 46(1) Notwithstanding any other Act or any privilege that is available at law including solicitor client privilege, the commissioner may, in a review **<u>or investigation</u>**, require to be produced and examine any personal health information that is in the custody or control of a trustee.
>
> (2) For the purposes of conducting a review **<u>or investigation</u>**, the commissioner may summon and enforce the appearance of persons before the commissioner and compel them to give oral or

written evidence on oath or affirmation and to produce any documents or things that the commissioner considers necessary for a full review, in the same manner and to the same extent as the court.

(3) For the purposes of subsection (2), the commissioner may administer an oath or affirmation.

2. Right to Set Procedures

Manitoba's PHIA contains a provision that gives the Ombudsman the right to set his or her own procedures as follows:

Procedures for a review
48.4(1) The adjudicator may make rules of procedure for conducting a review under section 48.3.

In *It's Time to Update*, I proposed the following amendment to FOIP:

XX Subject to this Act, the Commissioner may determine the procedure to be followed in the performance of any duty or function of the Commissioner under this Act.

Proposal

Proposed is the inclusion of the following language in HIPA:

45(4) The commissioner may make rules of procedure for conducting a review or investigation.

3. Right of Entry

This office has the ability to enter any premises as part of its powers under FOIP but not HIPA. Manitoba's PHIA contains the following provision:

Right of entry
30 Despite any other enactment or any privilege of the law of evidence, in exercising powers or performing duties under this Act, the Ombudsman has the right,

(a) during regular business hours, to enter any premises of a trustee in which the Ombudsman believes on reasonable grounds there are records relevant to an investigation and examine and make copies of them; and

(b) to converse in private with any officer, employee or agent of the trustee.

Similarly, Newfoundland and Labrador's PHIA states the following:

70. (1) In conducting a review, and notwithstanding another Act or regulation or a privilege under the law of evidence, the commissioner may, where he or she reasonably believes that the premises contains a book, record or other document relevant to the subject-matter of the review, without a warrant or court order,

(a) enter a premises to view or inspect the premises;

PIPEDA's related provision is as follows:

> 12.1 (1) In the conduct of an investigation of a complaint, the Commissioner may
>
> (a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record;
>
> (b) administer oaths;
>
> (c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;
>
> (d) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises;
>
> (e) converse in private with any person in any premises entered under paragraph (d) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and
>
> (f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the investigation.

And, finally, from Ontario's PHIPA is the following:

> **Inspection powers**
> 60. (1) In conducting a review under section 57 or 58, the Commissioner may, without a warrant or court order, enter and inspect any premises in accordance with this section if,
>
> (a) the Commissioner has reasonable grounds to believe that,
>
> (i) the person about whom the complaint was made or the person whose activities are being reviewed is using the premises for a purpose related to the subject-matter of the complaint or the review, as the case may be, and
>
> (ii) the premises contains books, records or other documents relevant to the subject-matter of the complaint or the review, as the case may be;
>
> (b) the Commissioner is conducting the inspection for the purpose of determining whether the person has contravened or is about to contravene a provision of this Act or its regulations; and
>
> (c) the Commissioner does not have reasonable grounds to believe that a person has committed an offence.

Our FOIP contains the following language:

> **Powers of commissioner**
> 54(1) Notwithstanding any other Act or any privilege that is available at law, the commissioner may, in a review:
>
> ...
>
> (b) enter and inspect any premises occupied by a government institution.

Proposal

It is proposed that similar wording be added to HIPA as contained in FOIP as follows:

> 46(4) Notwithstanding any other Act or any privilege that is available at law, the commissioner may, in a review or investigation enter and inspect any premises occupied by a trustee.

4. Disclosures by Commissioner

There are circumstances in which it may be necessary for the Commissioner to exercise his discretion and disclose limited information in certain situations. In this regard, Alberta's HIA includes the following provision:

> 91(3.2) The Commissioner may disclose any information to any person where the Commissioner reasonably believes the disclosure of the information to that person
>
> (a) is necessary to protect the privacy, health or safety of an individual, or
>
> (b) is in the public interest.

PIPEDA also allows for disclosure if in the public interest as follows:

> 20. (2) The Commissioner may, if the Commissioner considers that it is in the public interest to do so, make public any information that comes to his or her knowledge in the performance or exercise of any of his or her duties or powers under this Part.

Proposal

It is proposed that section 54 of HIPA be amended as follows:

> 54(7) The Commissioner may disclose any information to any person where the Commissioner reasonably believes the disclosure of the information to that person
>
> (a) is necessary to protect the privacy, health or safety of an individual, or
>
> (b) is in the public interest.

W. Additional Offences and Penalties

The following HIPA amendments came into force June 1, 2016:

> 64(1.1) No trustee or information management service provider, or former trustee or information management service provider, shall fail to keep secure the personal health information in its custody or control as required by this Act.
>
> (1.2) No person shall be found to have contravened subsection (1.1) if that person can establish that he or she took all reasonable steps to prevent the contravention.
>
> ...
>
> (3.1) An individual who is an employee of or in the service of a trustee or information management service provider and who knowingly discloses or directs another person to disclose personal health

information in circumstances that would constitute an offence by the trustee or information management service provider pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the trustee or information management service provider has been prosecuted or convicted.

(3.2) An individual who is an employee of or in the service of a trustee and who wilfully accesses or uses or directs another person to access or use personal health information that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the trustee has been prosecuted or convicted.

(3.3) An individual who is an employee of or in the service of an information management service provider and who wilfully accesses or uses or directs another person to access or use personal health information for a purpose that is not authorized by subsection 18(1) of this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the information management service provider has been prosecuted or convicted.

Other offense provisions could be added. For instance, Alberta's HIA contains the following provisions:

Offences and penalties
107(2) No person shall knowingly

(a) collect, use, disclose or create health information in contravention of this Act,

(b) gain or attempt to gain access to health information in contravention of this Act,

(c) make a false statement to, or mislead or attempt to mislead, the Commissioner or another person performing the duties, powers or functions of the Commissioner or other person under this Act,

(d) obstruct the Commissioner or another person in the performance of the duties, powers or functions of the Commissioner or other person under this Act,

…

(3) No researcher shall knowingly breach the terms and conditions of an agreement entered into with a custodian pursuant to section 54.

(4) No information manager shall knowingly breach the terms and conditions of an agreement entered into with a custodian pursuant to section 66.

Nova Scotia's PHIA contains the following unique offense provision:

106 A person is guilty of an offence if the person

…

(m) breaches the terms and conditions of an agreement entered into with a custodian under this Act.

Proposal

HIPA does not presently include any specific offense provisions similar to those underlined above. The additional amendments proposed would provide as follows:

> 64(1) No person shall
>
> …
>
> (g) knowingly collect, use, disclose or create personal health information in contravention of this Act,
>
> (h) knowingly gain or attempt to gain access to personal health information in contravention of this Act
>
> ...
>
> (3.4) Any researcher that knowingly breaches the terms and conditions of a written agreement entered into with a trustee pursuant to section 29 is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the information management service provider has been prosecuted or convicted.

X. Review of HIPA

Many access and privacy laws in Canada contain a statutory requirement for a review by a legislative committee after a fixed period of three or five years. HIPA does not. An example of one that does is Alberta's HIA which contains the following provision:

> **Review of Act**
> 109(1) A special committee of the Legislative Assembly must begin a comprehensive review of this Act within 3 years after the coming into force of this section and must submit to the Legislative Assembly, within one year after beginning the review, a report that includes the committee's recommended amendments.
>
> (2) The review referred to in subsection (1) must include a review of the application of this Act
>
> (a) to departments of the Government of Alberta,
>
> (b) to local public bodies as defined in the Freedom of Information and Protection of Privacy Act, and
>
> (c) to any other entity that is not a custodian and has information about the health of an individual in its custody or under its control.

Proposal

It is proposed that there is a statutory review of HIPA every five years. In *It's Time to Update*, this office proposed the following wording which is proposed for inclusion in HIPA as well:

XX After five years, after the coming into force of this Act and every five years thereafter, the minister responsible for this Act shall refer it to a committee for the purpose of undertaking a comprehensive review of the provisions and operations of this Act.

Y. Inter-jurisdictional Investigations

In relation to an investigation of a potential privacy breach involving an interoperable EHR, this office should have the ability to collaborate on investigations with oversight bodies in other jurisdictions. HIPA should allow my office to share information with Information and Privacy Commissioners in other jurisdictions where necessary to undertake a joint or at least coordinated investigation where more than one jurisdiction's health information law is engaged. As personal health information moves over provincial borders, eventually there will be a need to conduct an investigation into a related privacy breach. It will require collaboration with the oversight office in a different jurisdiction.

HIPA requires a provision that allows the Commissioner to share information about matters within his jurisdiction with the Commissioner(s) in other jurisdictions where more than one jurisdiction is involved. There are currently strict confidentiality requirements in FOIP, LA FOIP and HIPA that constrain this office from sharing case file information with the oversight agency elsewhere.

The provision in Alberta's HIA is as follows:

> **General powers of Commissioner**
> 84(1) In addition to the Commissioner's powers and duties under Divisions 1 and 2 with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure its purposes are achieved, and may
>
> …
>
> (j) exchange information with an extra-provincial commissioner and enter into information sharing and other agreements with extra-provincial commissioners for the purpose of co-ordinating activities and handling complaints involving 2 or more jurisdictions.
>
> (2) For the purposes of subsection (1)(j), "extra-provincial commissioner" means a person who, in respect of Canada or in respect of another province or territory of Canada, has duties, powers and functions similar to those of the Commissioner.

Yukon's HIPMA contains the following:

> **General powers of commissioner**
> 92 In addition to the specific duties and powers assigned to the commissioner under this Act, the commissioner is responsible for overseeing how this Act is administered to ensure that its purposes are achieved, and may
>
> …
>
> (f) exchange personal information and personal health information with any person who, under legislation of another province or Canada, has powers and duties similar to those conferred upon the commissioner under this Act or the Access to Information and Protection of Privacy Act;

(g) enter into information-sharing agreements for the purposes of paragraph (f) and into other agreements with the persons referred to in that paragraph for the purpose of coordinating their activities and exercising any duty, function or power conferred on the commissioner under this Act; and

(h) perform any prescribed duties or functions or exercise any prescribed power.

Ontario's PHIPA includes the following but is not as clear:

General powers
66. The Commissioner may,

…

(e) assist in investigations and similar procedures conducted by a person who performs similar functions to the Commissioner under the laws of Canada, except that in providing assistance, the Commissioner shall not use or disclose information collected by or for the Commissioner under this Act;

PIPEDA contains the following language:

23. (1) If the Commissioner considers it appropriate to do so, or on the request of an interested person, the Commissioner may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with any person who, under provincial legislation, has functions and duties similar to those of the Commissioner with respect to the protection of such information.

(2) The Commissioner may enter into agreements or arrangements with any person referred to in subsection (1) in order to

(a) coordinate the activities of their offices and the office of the Commissioner, including to provide for mechanisms for the handling of any complaint in which they are mutually interested;

(b) undertake and publish research or develop and publish guidelines or other instruments related to the protection of personal information;

(c) develop model contracts or other instruments for the protection of personal information that is collected, used or disclosed interprovincially or internationally; and

(d) develop procedures for sharing information referred to in subsection (3).

(3) The Commissioner may, in accordance with any procedure established under paragraph (2)(d), share information with any person referred to in subsection (1), if the information

(a) could be relevant to an ongoing or potential investigation of a complaint or audit under this Part or provincial legislation that has objectives that are similar to this Part; or

(b) could assist the Commissioner or that person in the exercise of their functions and duties with respect to the protection of personal information.

(4) The procedures referred to in paragraph (2)(d) shall

(a) restrict the use of the information to the purpose for which it was originally shared; and

(b) stipulate that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner.

Proposal

Just as it was proposed in *It's Time to Update*, similar language is proposed for HIPA as follows:

> XX(1) In addition to the Commissioner's powers and duties in this Act, the Commissioner is generally responsible for monitoring how this Act is administered to ensure its purposes are achieved, and may exchange information with an extra-provincial commissioner and enter into information sharing and other agreements with extra-provincial commissioners for the purpose of co-ordinating activities and handling complaints involving two or more jurisdictions.
>
> (2) For the purposes of subsection (1), "extra-provincial commissioner" means a person who, in respect of Canada or in respect of another province or territory of Canada, has duties, powers and functions similar to those of the Commissioner.

Z. Whistleblower Protection

It is recommended that a whistleblower provision be included in HIPA along the lines of similar provisions in British Columbia especially noting that *The Public Interest Disclosure Act* does not apply to trustees. The provision in British Columbia's *Freedom of Information and Protection of Privacy Act* provides as follows:

> 30.3 An employer, whether or not a public body, must not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee of the employer, or deny that employee a benefit, because
>
> (a) the employee, acting in good faith and on the basis of reasonable belief, has notified the minister responsible for this Act under section 30.2,
>
> (b) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the commissioner that the employer or any other person has contravened or is about to contravene this Act,
>
> (c) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order to avoid having any person contravene this Act,
>
> (d) the employee, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention of refusing to do anything that is in contravention of this Act, or
>
> (e) the employer believes that an employee will do anything described in paragraph (a), (b), (c) or (d).

PIPEDA also contains whistleblower related provisions as follows:

> 27. (1) Any person who has reasonable grounds to believe that a person has contravened or intends to contravene a provision of Division 1, may notify the Commissioner of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.
>
> (2) The Commissioner shall keep confidential the identity of a person who has notified the Commissioner under subsection (1) and to whom an assurance of confidentiality has been provided by the Commissioner.
>
> 27.1 (1) No employer shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee, or deny an employee a benefit of employment, by reason that
>
> (a) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that the employer or any other person has contravened or intends to contravene a provision of Division 1;
>
> (b) the employee, acting in good faith and on the basis of reasonable belief, has refused or stated an intention of refusing to do anything that is a contravention of a provision of Division 1;
>
> (c) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order that a provision of Division 1 not be contravened; or
>
> (d) the employer believes that the employee will do anything referred to in paragraph (a), (b) or (c).
>
> (2) Nothing in this section impairs any right of an employee either at law or under an employment contract or collective agreement.
>
> (3) In this section, "employee" includes an independent contractor and "employer" has a corresponding meaning.

Another example is from Newfoundland and Labrador's PHIA as follows:

> **Non-retaliation**
> 89. A person shall not dismiss, suspend, discipline, demote, harass or otherwise disadvantage or penalize an individual where
>
> (a) the individual, acting in good faith and on the basis of reasonable belief, has disclosed to the commissioner that another person has contravened or is about to contravene a provision of this Act or the regulations;
>
> (b) the individual, acting in good faith and on the basis of reasonable belief has done or stated an intention of doing an act that is required to be done in order to avoid having a person contravene a provision of this Act or the regulations;
>
> (c) the individual, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention to refuse to do an act that is in contravention of this Act or the regulations; or
>
> (d) another person believes that the individual will do an act described in paragraph (a), (b) or (c).

Proposal

Proposed is the introduction of a provision similar to that found in Newfoundland and Labrador as follows:

Non-retaliation

X A trustee shall not dismiss, suspend, discipline, demote, harass or otherwise disadvantage or penalize an individual where

(a) the individual, acting in good faith and on the basis of reasonable belief, has disclosed to the commissioner that another person has contravened or is about to contravene a provision of this Act or the regulations;

(b) the individual, acting in good faith and on the basis of reasonable belief has done or stated an intention of doing an act that is required to be done in order to avoid having a person contravene a provision of this Act or the regulations;

(c) the individual, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention to refuse to do an act that is in contravention of this Act or the regulations; or

(d) another person believes that the individual will do an act described in paragraph (a), (b) or (c).