

# HEALTH RECORDS PROTECTION REPORT

April 2014

Report of Saskatchewan's Health  
Records Protection Working Group  
to the Deputy Minister of Health



# Table of Contents

<b>Executive Summary .....</b>	<b>1</b>
<b>Introduction and Background.....</b>	<b>3</b>
<b>(a) Background.....</b>	<b>3</b>
<b>(b) Health Records Protection Working Group.....</b>	<b>3</b>
<b>Issues Identified by Working Group.....</b>	<b>5</b>
<b>(a) Enforcement of HIPA.....</b>	<b>5</b>
<b>(b) Possible “Gaps” in HIPA.....</b>	<b>5</b>
<b>(c) Abandoned Records Problem .....</b>	<b>5</b>
<b>Jurisdictional Review of Issues .....</b>	<b>6</b>
<b>Working Group Outcomes .....</b>	<b>7</b>
<b>(a) Aids to Enforcement of <i>The Health Information Protection Act</i> .....</b>	<b>7</b>
<b>(b) Possible Gaps in HIPA.....</b>	<b>10</b>
<b>(c) Patient Record Storage Solutions.....</b>	<b>16</b>
<b>Summary and Conclusion .....</b>	<b>21</b>
<b>Appendix A: Jurisdictional Scan .....</b>	<b>22</b>



# Executive Summary

The Health Records Protection Working Group (Working Group) was established in September 2012 by the Ministry of Health for the purpose of examining the following issues and reporting their findings and recommendations to the Deputy Minister of Health:

- a. the mechanisms for enforcement of trustee responsibilities to protect patient records as required under *The Health Information Protection Act* (HIPA). The Working Group will review not only the current enforcement mechanisms, but also comment on specific changes which may be desired to clarify trustee responsibilities or to assist in achieving trustee compliance with HIPA; and
- b. specific changes which will prevent abandonment of patient records, thereby protecting patient confidentiality and reducing events requiring need for enforcement.

The Working Group undertook a series of meetings to address the issues and conducted multi-jurisdictional research to determine how similar issues are addressed in other provinces. The Working Group analyzed the underlying causes of the issues raised and the differences in approach undertaken in other jurisdictions and provided the following 11 recommendations for the Ministry of Health to consider to address the issues identified.

## Recommendations

1. **Strict liability offence.** The Working Group recommended that a strict liability offence provision should be added to HIPA specifically aimed at addressing abandoned records. This will forego the need to establish evidence of specific intent. When records are found abandoned, once the abandonment is established and the trustee determined, that trustee will have to show he/she took all reasonable steps to prevent the abandonment from occurring.
2. **Individual offence for willful disclosure of personal health information.** The Working Group recommended that provisions be added to make it clear that the offence provisions for intentional/willful disclosure of personal health information apply not only to trustees, but to individuals who are employees of trustees.
3. **Proposed snooping offence.** The Working Group recommended the addition of a specific offence for inappropriate use of personal health information by employees of a trustee who access information without a need for that information (snooping).
4. **Gaps in definition of trustee for physician practice arrangements.** The Working Group recommended that the Government take one of two actions to address some forms of physician clinic practice arrangements currently being utilized, which HIPA does not contemplate. The Working Group concluded that the definition of trustee under the Act does not apply to these arrangements and recommended:
  - (a) Regulations be passed under HIPA to make the clinic operators that control patient records trustees;or

- (b) the practice arrangements be precluded by:
    - (i) making legislative changes to HIPA to make the physician responsible for the records notwithstanding the arrangements;
    - (ii) making legislative changes to *The Medical Professions Act, 1981* clearly precluding these types of operating structures.
5. **Proclaim sections of HIPA.** The Working Group recommended that subsections 17(1), and subsections 18(2) and (4) of HIPA be proclaimed into force. These provisions require trustees to have record retention/destruction policies and written contracts with information management service providers.
  6. **Take control of abandoned records.** The Working Group recommended that a system be put in place to quickly respond to a discovery of abandoned records and to take control of the records. A new provision should be added to HIPA authorizing the Minister of Health to appoint a person to take over control and custody of the records where an active trustee abandons records.
  7. **Single repository for abandoned records.** The Working Group recommended that there should be one facility where abandoned records associated with an unknown or unavailable trustee are taken. The Working Group determined that the operator of the existing electronic health record system, eHealth Saskatchewan, would be the most appropriate party to be that repository.
  8. **Enact regulations governing designated archives.** The Working Group recommended that Government pass the remaining regulations contemplated by section 63(1) (k) of HIPA to complete the responsibilities of designated archives for dealing with records transferred by trustees.
  9. **Designated archives required to accept records.** The Working Group recommended at least one of the designated archives should be required to accept records offered by trustees. Ideally, that archive might be eHealth Saskatchewan, however, it is possible to designate that particular designated archives be required to accept records from particular trustees.
  10. **Private record storage solutions be available.** The Working Group recommended Government consider permitting private records storage and processing companies with sound privacy practices to be considered for listing in the regulations as designated archives to provide for more options for transferring patient records.
  11. **Designated archive storage costs borne by trustees.** The Working Group recommended that the costs associated with transferring and storing with a designated archive be the responsibility of the trustee. A system should be developed to ensure that the funds required covering the costs of the designated archive services are paid by the trustee in some fashion. The Working Group is not unanimous on how this would be accomplished, but the discussion noted the following:
    - (a) For trustees that are regulated by a professional association, the professional association could levy annual fees from the members and set up a fund to cover the costs associated with record storage where records are abandoned by their members.
    - (b) Trustees licensed to carry on their health operations could be required to demonstrate that they have an arrangement or plan to deal with patient records on winding up operations. Additional licensing fees could be assessed for the purposes of establishing a fund that the licensing body can access in the event records of an operator are abandoned.

# Introduction and Background

## (a) Background

In March 2011, a large number of patient files were found in a recycling bin behind the Albert Park Medical Clinic in South Regina. A member of the public noticed the records and notified their member of the legislature as well as the Office of the Information and Privacy Commissioner of Saskatchewan (OIPC). The OIPC took control of the records and began an investigation into the issue. On July 14, 2011 the OIPC released its public report on the matter (<http://www.oipc.sk.ca/Reports/IR%20H-2011-001.pdf>).

In summary, the OIPC found that the records at issue belonged to the Albert Park Family Medical Clinic and that the trustee of that Clinic under *The Health Information Protection Act* (HIPA) was Dr. Teik Im Ooi. In the opinion of the OIPC, Dr. Ooi failed to meet the requirements of section 16 of HIPA, which requires trustees to have in place written policies and procedures to adequately safeguard patients' personal health information and failed to put in place agreements and mechanisms required by section 18 in dealings with the Information Management Service Providers (IMSP) who provided storage, transportation and destruction of personal health information. As a result of the findings, the OIPC made 11 recommendations to deal with the matter, including a recommendation that the Minister of Justice consider commencing a prosecution of Dr. Ooi pursuant to section 64 of HIPA.

In response to this recommendation, the Ministries of Health and Justice arranged for a further investigation of the incident to be conducted by the investigative unit of the Ministry of Government Services to gather the evidence required to consider prosecution. The evidence obtained was reviewed by the Public Prosecutions Division of the Ministry of Justice and by a private law firm to determine if charges were warranted under HIPA. Both reviews concluded that there was not enough evidence to pursue an offence as it is described under HIPA. Offences under the Act required proof that the trustee was aware that the safeguards which the trustee had in place were inadequate to meet appropriate standards, which was difficult in this case since the records were in storage and the trustee did not remove the records nor cause the patient files to be placed in the dumpster. No charges were pursued.

While a prosecution was not appropriate in this matter, the Government was concerned that the requirements for an offence under HIPA to be established may not be appropriate and directed that a Working Group be established to examine the matter.

## (b) Health Records Protection Working Group

In response to the Government's direction, in September 2012 the Health Records Protection Working Group (Working Group) was established with the following mandate:

- (i) To examine and provide advice on the mechanisms for enforcement of trustee responsibilities to protect patient records as required under HIPA. The Working Group will review not only the current enforcement mechanisms, but also comment on specific changes which may be desired to clarify trustee responsibilities or to assist in achieving trustee compliance with HIPA; and

- (ii) To examine and recommend specific changes which will prevent abandonment of patient records, thereby protecting patient confidentiality and reducing events requiring need for enforcement.

The Working Group is made up of representation from the following:

- Ministry of Health
- Ministry of Justice and the Attorney General
- Saskatchewan College of Physicians and Surgeons
- Saskatchewan Registered Nurses Association
- Saskatchewan College of Pharmacists
- Saskatchewan Medical Association
- Patient interests representative

The Working Group's function was to prepare a report on its mandate and to provide its analysis and written recommendations to the Deputy Minister of Health.



## Issues Identified by Working Group

The Working Group's discussions focused on three main areas:

### (a) Enforcement of HIPA

The primary discussions of the group focused on the current enforcement mechanisms within HIPA and whether the existing mechanisms are adequate to help ensure trustee compliance with the legislation. We undertook an analysis of the existing offence provisions within HIPA, the evidentiary requirements necessary to be proven to establish an offence and the practical issue of who collects the evidence required. In conducting the analysis, the Working Group referenced the approaches used in other jurisdictions. A copy of the jurisdictional scan has been attached to this report as Appendix A: Jurisdictional Scan.

### (b) Possible "Gaps" in HIPA

During the Working Group's discussion, a number of separate issues emerged around whether there were some gaps in HIPA that needed to be addressed in order to clarify trustee responsibilities and the Act's application. The group raised questions as to whether the definition of trustee in the Act was sufficient to apply to certain physician clinic practice arrangements, and in particular, whether patient records in those clinics were governed by HIPA. The group also noticed that some provisions of HIPA dealing with trustee contracts with information management service providers had not been proclaimed in force and examined whether these provisions should now be operational.

### (c) Abandoned Records Problem

The Working Group discussed the challenge associated with dealing with records that are found abandoned, including taking control of those records and finding appropriate repositories so that personal health information can be available to patients but still remain secure. The group noted that, while there should not be a circumstance where records are found abandoned, such incidents continue to occur notwithstanding the clear responsibilities trustees have to protect those records. While human error can occur, the number of cases where records are found to be improperly stored or destroyed is troubling and indicates that there may be a lack of education, understanding and clear procedure in place within some trustee operations. In addition, there are a variety of circumstances including death, retirement, change of practice or relocation of a trustee which if not properly handled, can expose patient medical records to privacy and security risks. While HIPA contemplates that there should be designated archives where trustees can deliver patient records for storage when they cease to practice, this system has not proven to be effective. Therefore, the Working Group concluded that changes should be made to develop a more effective records repository solution, which would assist in preventing abandoned records, and be available to maintain records which might be found abandoned. This solution, however, is not intended to negate the trustee's obligations with respect to records management, nor is it intended as an option of first resort.

## Jurisdictional Review of Issues

A review of how other jurisdictions deal with the issues identified by the Working Group was undertaken. Many provinces have laws governing personal health information, all of which have the same basic functions of providing for rules governing the collection, use and disclosure of personal health information, as well as providing for rights of individuals to access their own personal health information.

The jurisdictional scan considered affiliates and other bodies; responsibilities and compliance methods; unauthorized access/use of personal health information; mismanaged or abandoned records and existing offences/penalties and enforcement approaches; designated archives and information management service providers, strict liability considerations and the education or training provided to trustees/custodians. Refer to Appendix A: Jurisdictional Scan for summarized results of the environmental scan.

# Working Group Outcomes

## (a) Aids to Enforcement of the Health Information Protection Act

The Working Group recognizes that enforcement measures are the last resort; it means that an inappropriate disclosure has already occurred. Enforcement under HIPA and enforcement by the professional regulatory authority with respect to the members can be effective only as a key aspect of promoting ongoing compliance with professional and legislative requirements. If compliance is indeed our goal then any changes to HIPA must promote this end; charging individuals or corporations with an offence is not an end in and of itself. Simply put, we cannot charge our way out of a problem with abandoned health records. With that being said, the Working Group does however feel strongly that changes can be made to clarify the intent of the Act and better promote responsible compliance by all parties.

The proposed changes are intended to sharply focus the compliance requirements and clarify the policy position with respect to securing personal health information. These changes will assist in highlighting the consequences of non-compliance and bringing home the intended deterrent to trustees and their employees. When combined with a re-invigorated commitment from the professional regulatory authority to informing their members of their professional responsibilities regarding health records and appropriate by-law enforcement by the professions, these amendments can serve to tighten any gaps in the health record protection net. The jurisdictional review indicates a level of responsibility and engagement by professional regulatory authority's not reflected in Saskatchewan in certain key sectors. Expressly mandating professional responsibility, rather than simply empowering it, may also merit additional consideration.

### (i) Strict Liability Offence

The Working Group recommends that HIPA be amended to provide for a new strict liability offence specifically aimed at addressing the issue of abandoned Personal Health Information (PHI). Our legislative review reflects that this proposed provision would be unique to Saskatchewan. The Working Group is, nevertheless, of the view that it is important in this context to make a clear statement to trustees and information service providers that a failure to protect PHI will constitute a *prima facie* offence unless they can establish that they have taken all reasonable steps to prevent that contravention.

While it is beyond the Working Group's capacity and function to draft legislative provisions, in order to help to convey the intent of the Working Group's recommendations, suggestions for what might be included in the language of the offence provision are included in the Report. In regard to a strict liability offence provision, suggested language to consider appears below:

**64 (1.1)** *No trustee or information management service provider, or former trustee or information management service provider, shall abandon or otherwise manifestly fail to protect the confidentiality of personal health information.*

*1.2 No person shall be found to have contravened subsection (1.1) if that person can establish that they took all reasonable steps to prevent the contravention.*

*(2) Every person who contravenes subsection (1) or (1.1) ...*

This provision would be unique in that it moves beyond the specific intent required elsewhere in the Act necessary to constitute an offence. In other words, it is not enough for a trustee to assert that they did not intend for PHI to be abandoned; they must show that they took all reasonable steps to avoid having PHI abandoned.

If they are able to establish that they took all reasonable steps, then they will have a substantive defence to a charge under this new section. The Working Group feels that this is consistent with the public policy goals intended to address this issue. Negligence, incompetence or simple indifference should not be enough to defeat a charge of abandoning or manifestly failing to protect PHI in accordance with requirements of HIPA. Due diligence is required from every trustee or information management service provider that is entrusted with PHI in Saskatchewan. This new offence would both reflect and support that policy.

## **(ii) Individual Accountability**

The jurisdictional review of comparable legislation reflected that some other jurisdictions have specifically included an offence for individuals who as employees or agents of the trustee willfully disclose PHI without authorization. The Working Group understands that the existing offence provisions of HIPA permit such a charge to be laid against employees in appropriate circumstances. However, the Working Group believes, as a matter of general deterrence, it is essential that intentional violations of the spirit and intent of the Act carry with it appropriate sanctions, therefore, any question as to whether HIPA authorizes such charges should be removed. Accordingly, the Working Group recommends including a similar provision in HIPA as exists in other jurisdictions (refer to Appendix A: Jurisdictional Scan) to reinforce the individual responsibility that employees of trustees and information service providers bear when dealing with PHI. Where a trustee has not authorized disclosure and such disclosure would constitute an offence for the trustee, it should also clearly constitute an offence for that individual. Suggested language to consider for such an amendment might be:

**64 (3.1)** *An individual who is an employee of or in the service of a trustee or information management service provider and who, without the authorization of the trustee or information management service provider, willfully discloses personal health information in circumstances that would constitute an offence by the trustee or information management service provider under 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.*

## **(iii) Proposed Unauthorized Access by Individuals Offence Provision**

The Working Group has given serious consideration to recommending another unique individual offence: an offence for “snooping.” This is an important issue as it reflects the central policy intent in HIPA that PHI only be accessed and used by a trustee for a purpose expressly permitted by HIPA. There is limited precedent in Canada for an offence of this nature focused on individual conduct by an employee or agent of a trustee or an information service provider. In Manitoba, Bill 4 has recently been passed in order to address this issue. Creating an offence that focuses on the individual rather than the trustee may raise the concern of shifting the focus to individual employees rather than focusing on management and executive responsibility for institutional compliance. Rather than serving as a specific deterrent, such a provision could become an unwelcome complication in promoting overall

compliance. Nevertheless, the Working Group recommends the addition of a specific offence for inappropriate use of personal health information by employees of trustees who access personal health information without a need for that information.

An **unauthorized access by individuals'** offence could mirror the proposed 64 (3.1) as follows:

*3.2 An individual who is an employee of or in the service of a trustee and who, without the authorization of the trustee, wilfully accesses 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 or information management service provider 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, without the authorization of the information management service provider, wilfully accesses 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 trustee or information management service provider has been prosecuted or convicted.*

#### **(iv) Investigation/enforcement**

As noted above, clarity in promoting compliance and general deterrence are the central functions of offence provisions in non-criminal legislation. They serve to promote positive conduct rather than punish offensive conduct. The goal is to ensure compliance with HIPA and the protection of PHI. However, the proposed creation of new offences in HIPA also raises the issue of how investigation and enforcement of the provisions of the Act are conducted. There are a number of investigative possibilities with overlapping responsibilities, and it is important to understand how they interact with offences.

In general where concerns of a trustee's handling of PHI exist, complaints are first raised with the Office of the Information and Privacy Commissioner (OIPC). The OIPC is given power under HIPA to receive such complaints and conduct investigations into compliance with the Act's requirements. In order to conduct these investigations the Information and Privacy Commissioner is given significant power to compel production of records and information and to question individuals. These powers are necessary in order for the Commissioner to fulfill his role to investigate alleged breaches, reach conclusions on the matter and make recommendations as to what steps should be taken by a trustee to address the issue. However, in reaching these conclusions the Commissioner might be applying a different (lower) standard of proof that the Act's requirements have been breached than would be required to establish an offence. Equally, the ability of the Commissioner to require production of information as part of an investigation makes it questionable how much of the Commissioner's investigation could be used in a prosecution, where one has a right not to provide such information to investigators. Accordingly, the Commissioner's investigation is for a different purpose than prosecution. Its main function is for resolution of issues - determining validity of trustee practices and recommending methods to achieve better compliance. This is a very important and vital role for the Act's workings as most circumstances do not warrant prosecutorial sanction, but rather education and guidance.

Alongside the Commissioner's investigations are investigations that may be conducted either internally by a particular trustee when employees are alleged to have breached the Act, or by regulators of

particular professions (the College of Physicians and Surgeons, Saskatchewan Association of Registered Nurses, the College of Pharmacy, etc.). Each of these investigations has their own purposes. Employers do investigations to determine if the allegation is accurate and if so, whether disciplinary action, including termination of employment, is warranted. Professional regulatory authorities license and regulate the conduct of their members and can undertake investigations when there are allegations a member has violated a particular standard of practice or his or her duties of confidentiality. Where a complaint is founded, the association can discipline the member through placing conditions on continuing licensure, or suspending or cancelling the member's license to practice. Both of these mechanisms allow for appropriate action to be taken which can have a significant impact on an individual and address inappropriate practices and conduct.

All of these available investigatory/enforcement mechanisms are important and utilized to help ensure compliance with the Act as not every breach warrants prosecutorial consideration. However, where a breach is egregious, a prosecutorial investigation is merited. Investigations of this type are done by the police, but factually and of necessity such investigations are rare. This caused the Working Group to examine whether some specific investigatory resources are in place in other jurisdictions to address offences. The jurisdictional review reflected that no jurisdiction dedicates specific offence-related investigation/enforcement resources for similar legislation. It also reflected that one type of response will not fit all types of contraventions under the Act. All contraventions are to be treated seriously but few will be treated identically and it is the nature and extent of the alleged violation that will drive the response.

The Working Group is of the view that the widespread implementation of electronic medical records and electronic repositories of health information, moving from paper to electronic records, will be a significant tool to safeguard patient information. The new provision proposed in s22(3) will assist in getting PHI from A to B in cases where an existing trustee fails to properly secure PHI that was in their custody and control. In some cases the Minister can work with a local Regional Health Authority (RHA) or the appropriate profession to secure the PHI and either store it or return it to the responsible trustee. In others the PHI may be transferred from the trustee to an appropriate authority and the trustee can be sanctioned as a current or former trustee. Then, depending on the nature of the violation, the Ministry can work with the OIPC, the police, health officials, RHAs and the professions to ensure all parties are requiring trustees and members to meet their obligations under the Act and the professional bylaws.

Promoting ongoing compliance and, where necessary, conducting subsequent investigation and enforcement will remain a joint endeavor that must remain sufficiently flexible to respond to variant circumstances.

## **(b) Possible Gaps in HIPA**

### **(i) Definition of trustee in relation to physician practice arrangements**

Some medical clinics are operated by a business corporation which provides the space, employs the administration staff, and either employs or contracts with physicians to provide patient care. While physicians collect and record personal information about patients, they do not have custody or control of the patient records – as employees the records belong to the employing corporation. Where physicians are contracted by the operator, the contracts provide that physicians collect the information

but maintain no control over the patient records. When physicians leave these clinic arrangements the patient records remain with the clinic operator.

Similar arrangements are structured with municipalities where the municipality sets up a clinic practice and provides all operational support to help recruit physicians to set up in the community. When the physician leaves the municipality the records are retained by the municipality for the benefit of the patient and the next physician. Other situations involve medical or dental clinics or primary health clinics operated on reserve by Tribal Councils or individual Bands which is a significant concern by at least one of the Working Group members. HIPA does not specifically address these practice arrangements. Under HIPA, a trustee is one of a specific list of persons who have “custody or control” of personal health information. The definition of trustee in section 2 provides:

- (t) *“trustee” means any of the following that have custody or control of personal health information:*
  - (i) *a government institution;*
  - (ii) *a regional health authority or a health care organization;*
  - (iii) *a person who operates a special-care home as defined in The Housing and Special-care Homes Act;*
  - (iv) *a licensee as defined in The Personal Care Homes Act;*
  - (v) *a person who operates a facility as defined in The Mental Health Services Act;*
  - (vi) *a licensee as defined in The Health Facilities Licensing Act;*
  - (vii) *an operator as defined in The Ambulance Act;*
  - (viii) *a licensee as defined in The Medical Laboratory Licensing Act, 1994;*
  - (ix) *a proprietor as defined in The Pharmacy Act, 1996;*
  - (x) *a community clinic:*
    - (A) *as defined in section 263 of The Co-operatives Act, 1996;*
    - (B) *within the meaning of section 9 of The Mutual Medical and Hospital Benefit Associations Act; or*
    - (C) *incorporated or continued pursuant to The Non-profit Corporations Act, 1995;*
  - (xi) *the Saskatchewan Cancer Foundation;*
  - (xii) *a person, other than an employee of a trustee, who is:*
    - (A) *a health professional licensed or registered pursuant to an Act for which the minister is responsible; or*
    - (B) *a member of a class of persons designated as health professionals in the regulations;*
  - (xiii) *a health professional body that regulates members of a health profession pursuant to an Act;*
  - (xiv) *a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee;*
  - (xv) *any other prescribed person, body or class of persons or bodies;*

By and large business corporations providing medical services are not listed, nor are other forms of operation outside of the traditional physician operated clinic. Under the arrangements of concern, the medical practitioners do not have custody or control of the patient records – which is one of the requirements of the definition of trustee. Accordingly, even though a physician may collect the information and create the record, because the operator owns the record it is unlikely the physician would be found to be a trustee of that record under the current definition.

HIPA does include corporations which provide medical services as trustees under the Act. For example, community clinics are corporations and are listed as a trustee, operators under *The Ambulance Act* are

often business corporations as are many Personal Care Homes and they are trustees as well. These operators are different in nature from the ones under discussion however, as they are all in some fashion regulated in operation by another statute – their authority to exist and deliver health services is based in law.

The policy upon which HIPA was developed does not appear to have envisioned a clinic medical practice being operated by a corporation other than a physician-based professional corporation. HIPA does list physicians as trustees and appears to have envisioned that physicians would be the trustees in a clinical practice setting and would have custody and control of the personal health information and records in the clinic. While corporations could be set up to provide space and staff, they would only be an information management service provider in relation to patient records – the physician would not lose overall responsibility for the records.

However, for this policy to be effective, there must be a similar view/interpretation given by the College of Physicians and Surgeons (CPSS), the body that regulates physician practice, to the restrictions on practice in *The Medical Profession Act, 1981* or to acceptable standards of practice in relation to patient confidentiality and medical record keeping under the bylaws. CPSS does not interpret *The Medical Profession Act, 1981* as precluding this type of corporation structure nor does it consider that its bylaws prohibit physicians from entering into practice arrangements where they do not maintain custody or control of the personal health information that they collect and record. If this view continues and CPSS plays no regulatory role, then there is a gap. In a situation where a non-physician operator of a medical practice is employing physicians or contracting with physicians to provide service to patients of the clinic, and the operator owns the patient records created, there is likely no trustee for those records under HIPA.

It should be noted that simply because HIPA may not apply to the patient records in this situation does not mean that no legislation applies. In the case of a municipality that operates a medical clinic, the patient records would be governed by the personal information provisions set out in *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP). In the case of a business corporation that is operating a medical clinic or a band council operating on reserve, it appears likely that *The Personal Information Protection and Electronic Documents Act* (PIPEDA) will apply to the personal information within the records. So rules of confidentiality and access will continue to apply to the records.

Having HIPA apply makes the rules applicable to this information consistent and avoids confusion as to the applicable legislative regime. However, it is already the case that HIPA's rules do not apply to situations of all personal health information held in Saskatchewan – so essentially the issue is determining where the line should be drawn in relation to the application of legislation to the information. Insofar as these situations involve clinic settings with medical practitioners, the Working Group has arrived at the conclusion that HIPA's rules should apply, for the rules will then be consistent and practitioners will not need to attempt to learn and comply with two different legislative regimes.

While this issue is not widespread, it is believed that it is not uncommon either. CPSS has no accurate information on how physician practice structures are set up as it does not regulate those structures, but it has experienced problems in having physicians access patient records in such setting over a number of years and these problems do not appear to be lessening.

This operational issue is not unique to Saskatchewan, but how the matter is addressed varies by



jurisdiction. In Manitoba's *Personal Health Information Act* the definition of trustee includes a health professional or a health facility that "collects or maintains" personal health information. The word "maintain" is defined to mean to have "custody or control" of the information. Accordingly, the Manitoba definition will apply if a health professional or health facility collects the information – even without custody or control, which is broader than the definition in Saskatchewan and would conceivably apply to a health professional that collects the information in one of the situations in issue. In addition, the Manitoba legislation defines the term "health facility" to include "a medical clinic" and, while that phrase is vague, such is interpreted to include operations like the ones in issue in Saskatchewan.

However, Manitoba is currently reviewing with its professional regulatory authority in all situations where the practice of that profession is being conducted by a corporation (see Appendix A: Jurisdictional Scan). Under *The Manitoba Regulated Health Professions Act*, a corporation is precluded from carrying on the practice of a regulated health profession unless the corporation is authorized to do so in the regulations to the Act. That corporation could then be specifically known and dealt with as a trustee under Manitoba's *Personal Health Information Act*. If a similar provision existed in Saskatchewan, this would have a direct impact on the practice of medicine in the situations at issue and such practice situations could clearly not exist unless authorized in accordance with the statutory scheme. To make this rule as clear as it exists in Manitoba, changes to a number of professional regulatory statutes would need to be implemented as *The Manitoba Regulated Health Professions Act* is an umbrella piece of legislation under which all health professions that are regulated are governed and Saskatchewan has no similar legislation; rather it has specific profession-based legislation. Alberta's *Health Information Act* addresses this issue differently.

Alberta does not have a "custody or control" requirement in its definition of custodian. Rather, by being listed as a custodian under the legislation, that entity or person is bound by the duties which the Act provides in relation to the personal health information collected, used or disclosed by the custodian. Physicians are listed as custodians under the legislation as a health services provider that receives compensation under the Alberta Health Insurance Plan. *The Alberta Health Information Act* has a second definition of interest being an "affiliate." An affiliate is an individual employed by or in the service of a custodian. Affiliates have their own specific duties under the legislation, which are similar to those of trustees, but do not have the same responsibility for maintaining the records.

Where a physician is undertaking his/her own business operation, the physician would be a custodian under the Act. However, where the physician is in a practice situation as an employee or service provider to another custodian, then the physician would become an "affiliate" and have only the duties of an affiliate in relation to the information and records. Alberta advises that they consider physicians to be bound individually as custodians in these types of business practice arrangements and are to have policies and procedures in place within each clinic to determine how individual physicians will permit access to and disclosure of personal health information under his/her control as custodian. HIPA does not address this type of practice situation. For HIPA's rules to apply, one of two possible steps should be considered:

- I. Pass Regulations under HIPA to make the clinic operators that control patient records trustees.

Clause 2(t)(xv) of HIPA permits regulations to be enacted which expand the definition of trustee under the Act to include operators which are not currently listed. A new regulation could be passed

to make medical clinic operators who are not otherwise physicians or regulated health professionals, trustees under HIPA. This would result in HIPA applying to these operators and make physicians who leave clinic settings for new settings not responsible for the patient records that they created. Some care will need to be taken in drafting the regulation to ensure it is specific enough to identify operators bound by the rules and not too general to capture unintended operators. The Working Group recommends that if these types of relationships are permitted to continued, the gap should be addressed.

- II. Changes can be made to ensure in such clinic settings physicians remain responsible for the personal health information. This could occur in a number of fashions:
  - (i) through a legislative change to the definition of trustee under HIPA which removes the requirement for “custody or control” of personal health information, similar to that in Alberta. This change is significant, however, and likely requires further changes in the Act to incorporate the Alberta concept of “affiliate,” creating a lower level of duties on those who are employed or agents of trustees.
  - (ii) through a substantive legislative change to HIPA under which a regulated health professional remains responsible for the personal health information that the professional collects and records, and cannot transfer those responsibilities except to another trustee or to a designated archive. The Working Group notes that a similar result may be achievable with clear bylaws passed by CPSS which preclude physicians from transferring custody or control of medical records that they create except as authorized under HIPA.
  - (iii) Finally, an amendment could be made in *The Medical Profession Act, 1981* which clearly precludes the set up of operating structures for medical clinics which are not controlled by physicians. This may have some implications for current physician operating structures and some municipally run clinics.

The choice of which of the options to pursue is dependent upon the policy goal that is desired to be achieved. It is not for the Working Group to determine which policy is more appropriate, just to ensure that the issue is raised and solutions are proffered. The solutions raised will address the problem. The Working Group notes that some of the solutions raised require changes to statutes, which will take more time to achieve than non-legislative changes. As such, if the time period for resolution will be lengthy, taking an interim step like passing regulations which expand the definition of trustee to ensure that patient records are captured by HIPA would be appropriate. Furthermore, a mixture of the above options may be a viable solution.

## **(ii) Sections of HIPA Not Yet Proclaimed**

The Working Group noted that there continue to be some sections in HIPA which have not been proclaimed into force – in particular subsections 17(1), and subsections 18(2) and (4). The provisions provide:

**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.*

**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).

The Working Group was advised that these provisions were not proclaimed when HIPA became law to permit trustees an opportunity to develop the necessary policies dealing with retention and destruction of personal health information and to put in place with their information management service providers the required written agreements governing use, disclosure and storage of the information. Leaving these provisions unproclaimed will result in gaps in the protections which the Act is designed to provide.

Retention and destruction policies for records are relatively standard requirements for trustees of personal health information in legislation of jurisdictions across the country. Policies can be more effective than legislation in achieving positive results as policies are developed by the people who use the information and therefore help generate an understanding and ownership of the issue by trustees beyond what legislation can provide. Well-developed policies will have the effect of creating better understanding amongst trustees of the requirements of the Act and therefore assist in achieving compliance. Further, by developing retention policies, trustees will focus on the length of time that records need to be maintained, which should lead to more regular destruction of unnecessary personal health information and reduce the risk the information is lost or misplaced.

Subsections 18 (2) and (4) place specific duties on trustees to have written agreements in place with IMSPs and require those IMSPs to comply with those agreements. Again, these are key provisions to require trustees to think about how the personal health information they are collecting is being managed by IMSPs and to create clear rules on what the IMSP can do with that information. This not only creates legally enforceable obligations and contractual protections for both the trustee and the IMSP, but should also assist in making it clear what the obligations of each party are to avoid misunderstandings. Further, by proclaiming 18 (4), IMSPs will be legislatively required to comply with the terms of the agreement between it and the trustee, providing additional legislative protection and the possibility of enforcement through offence provisions if not followed. The jurisdictional scan noted that provisions requiring agreements to be in place with IMSPs are relatively standard across all jurisdictions.

It has been 10 years since HIPA was proclaimed in force and this may be an appropriate time to enact these sections. In the view of the Working Group, the absence of these provisions creates gaps in the protections the Act is intended to provide. The Working Group therefore recommends that the Government consider proclaiming these provisions of the Act in force.

## (c) Patient Record Storage Solutions

As part of its mandate the Working Group was asked to examine and recommend specific changes which will prevent the abandonment of patient records. Prevention is obviously the most beneficial goal, for if changes can be made which reduce situations of patient record abandonment, patient confidentiality is enhanced and the need for enforcement is reduced.

This report has previously provided recommendations such as providing for strict liability and individual offences which should assist in reducing incidents of abandonment of patient records through general deterrence. The Working Group notes, however, that there does not appear to be a good system in place to assist trustees who are leaving practice to provide secure storage and management for their records. As well, the Working Group believes that, where patient records are found abandoned, some practical issues exist which should be addressed surrounding obtaining control of and transferring control and management of the records. The Working Group's deliberations focused on two areas:

- i) Suggestions for addressing patient health records which are found abandoned; and
- ii) Identifying secure record retention and storage for trustees leaving their practice.

### (i) Suggestions for addressing patient health records which are found abandoned

The Working Group noted that events of abandonment should be reduced with the movement to the electronic health record systems operated by eHealth Saskatchewan. Most cases of abandonment involve large amounts of paper files, the existence of which should be significantly reduced as a result of moving to electronically based record systems. However, the movement to such a system will take time and paper records will continue to be held in significant numbers. Electronic records bring with them their own set of challenges in relation to security and implications for privacy which is beyond the scope of this report. Suffice it to say, however, that movement to this system should assist in reducing the number of incidents of abandoned records in the future.

Nonetheless, when situations of abandonment arise, there must be a system in place which can quickly respond to the issue and take control of the records. Once the records are secure, if there is no trustee for the records, there needs to be a place where the records can be taken to for safe handling. The Working Group believes that there should be a single facility where such records are taken. This would generate standard practices and efficiencies in handling these records by that provider, as well as give patients who may be impacted a consistent place to go to obtain their records.

The Working Group sought assistance from the Ministry of Health to determine who might best fit this role and who might have both capability and capacity to do so. Through discussion with the Ministry, the Working Group determined that the operator of the future electronic health record system, eHealth, would be the most appropriate party to be the repository. eHealth is designated as a trustee organization set out in the Act; it has background with the Act's requirements and is bound by the Act's rules. Further, as the electronic health records system provider, it will have the necessary authority and expertise to store records consistent with the requirements of the Act. Importantly, eHealth Saskatchewan will have the authority under HIPA as a trustee to store the records securely and provide access to patients who request access to their records.

In addition, the Working Group was concerned that there may be a gap in HIPA where patient records of an active trustee are found unsecured. Subsection 22(1) of HIPA currently creates an ongoing duty for

a former trustee to ensure that records containing PHI in their custody and control remain adequately secured. Subsection 22 (1) of HIPA does not apply if an active trustee fails to secure records. Subsection 22 (2) then authorizes the Minister of Health to appoint someone to take custody and control of the PHI where the former trustee has failed to do so. This will, with the new single storage solution outlined earlier and suggested to be adopted by eHealth, facilitate the timely transfer of abandoned PHI to be secured.

The Working Group has concluded that an additional subsection should be provided to fill the potential gap that could occur where a current active trustee (rather than a former trustee) fails to adequately secure PHI records that are in their custody or control. The new subsection would provide that the Minister may appoint a person or body to act in place of the trustee until custody or control of the personal health information is re-established, transferred to another trustee or transferred to an IMSP that is a designated archive. This provision would thus directly deal with a current trustee who is not meeting their responsibilities. When combined with the eHealth initiative, it will close any risk of a legal gap in the custody of these PHI records and allow the Minister to direct the trustee, eHealth, the Ministry, the professional regulatory authority, the RHA or any other entity that makes immediate sense to take temporary custody and control until it can be transferred to a new trustee or the original trustee can be informed of the breach and resume their responsibilities. Suggested language appears below:

***22 (2.1)** Where a trustee fails to carry out the duties imposed by this Act on a trustee with respect to personal health information in the custody or control of the trustee, the minister may appoint a person or body to act in place of the trustee until custody or control of the personal health information is re-established, transferred to another trustee or transferred to an information management service provider that is a designated archive.*

## **(ii) Identifying secure record retention and storage for trustees leaving their practice**

The Working Group noted that one of the main reasons for abandonment of patient records revolved around cessation of practice of a trustee for one reason or another. Examples are:

- trustees who retire from practice with no incoming trustee to take over the practice, or the incoming trustee does not want to take all of the former trustee's records;
- trustees who die unexpectedly leaving the records to the responsibility of the executor or administrator of his/her estate. In many instances the executor or administrator has no experience dealing with patient records or any idea of the requirements of HIPA that apply; and
- trustees who leave practice quickly and leave their records.

To examine the issue, the Working Group requested a jurisdictional scan be conducted to identify how other jurisdictions deal with patient records in circumstances where trustees exit practice arrangements. In all jurisdictions, the duty continued to fall upon the trustee to properly secure and maintain the records or to transfer the records to another trustee or IMSP. The jurisdictional scan noted the following:

- Various provincial professional regulatory authorities require trustees to inform them of where PHI records are stored. Additionally, many regulators require notification of where PHI will be stored, disposal steps/methods and if PHI will be transferred to another authorized trustee as a result of cessation of practice due to departure, death or termination from practice. The levels of

involvement of regulators vary amongst jurisdictions, and some jurisdictions (notably Alberta) place the responsibility to deal with abandoned patient records on the regulator associated with the particular professional involved.

- All jurisdictions permit trustees to transfer control of patient records to IMSPs. Some provinces officially authorize or “designate” an information management provider or a private records storage company to store PHI. Companies providing this service are not trustees or custodians and any instructions related to the PHI must come directly from trustees or custodians. This can be costly and time consuming as the trustee (or the executor) continues to have responsibility for the records, including the duty to provide access to records to patients who may request their information. If a trustee leaves the country or cannot be found, there is little ability for a patient to obtain those records.
- A few jurisdictions (including Saskatchewan) have provisions which permit trustees to transfer patient records to record repository agencies or archival services which then maintain the records and can use and disclose the information as authorized under the specific legislation. This is useful in permitting the records to still be available for patient access and permitting the trustee to remove themselves from responsibility for maintaining the records and complying with the Act’s duties.

HIPA has specific provisions (section 22) which are designed to address this issue by permitting trustees who are ceasing to be trustees to transfer patient records to successor trustees or to IMSPs that are prescribed in regulation to be designated archives. When such a transfer occurs the former trustee is relieved of future responsibility to deal with the records. Currently, the regulations list a number of organizations as designated archives that can accept trustee records, including Regional Health Authorities, the Ministry of Health, Saskatchewan Archives Board and health professional regulatory authorities. The Working Group noted that while this system is in place to address the problem, the reality would indicate that this system is not functioning properly to prevent abandonment of records. In the Working Group’s view the reasons may stem from the following:

- While designated archives exist, they are not required to accept records offered by a trustee who is exiting service. Rather, the designated archive must agree to accept the records. There is a significant cost associated with storage, cataloging and providing access to the records for a patient who requests them and few, if any, of the listed agencies appear willing to accept records because of this.
- When designated archives accept records, they are permitted to deal with them in accordance with the regulations. HIPA has provisions which permit enactment of regulations governing the duties of designated archives when records are accepted, including regulations outlining access rights, use and disclosure rules, requirements for storage and destruction and regulating costs. No such regulations are in place so only part of the system envisioned has been created. The rules applicable to designated archives when they have records are not set.
- None of the designated archives currently listed include private records storage solutions which may be available to be used by trustees and which are utilized in other jurisdictions. The Working Group believes that completion of the regulatory rules associated with the role of a designated archive, including where records can be stored, how PHI can be accessed and used, the period for

which records are required to be maintained and the costs which could be charged for accessing records by designated archives would assist these types of companies to develop a business case to provide service in Saskatchewan. In order for this to occur, however, the Government must be willing to list such companies as designated archives in the Regulations.

- Designated archives will have significant costs in storage of records, cataloguing and providing access to records at a patient's request. As there is no public funding for these services, trustees must bear these costs and may not be willing to do so. Accordingly, for the system to be successful it must have a mechanism for addressing the cost or for requiring the designated archive to accept the records.

The Working Group is of the view that the designated archive process set up by the Act is sound and that, if the above problems can be addressed, it should assist in preventing patient record abandonment by providing trustees with a solution to transfer patient records when they exit practice. To address the foregoing matters the Working Group makes the following recommendations:

- 1) Government should pass the remaining regulations contemplated by section 63(1)(k) of HIPA to complete the responsibilities of designated archives for dealing with records transferred by trustees. When creating these rules, consideration should be given not only to the appropriate duties to place on designated archives, but also the costs associated with the standards developed. For example, consideration might be given to lesser retention periods for designated archives to reduce storage costs.
- 2) At least one of the designated archives should be required to accept records offered by trustees. Ideally, that archive might be the same one that is contemplated in the recommendations which follow dealing with found patient records (eHealth). eHealth is contemplated to be the electronic health record system provider, and therefore having trustee patient records transferred to eHealth with the possibility of being electronically incorporated into existing patient records benefits the patient and makes the duties on the archive to find and retrieve patient information easier. However, there are other options. It is possible to designate that particular designated archives accept records from particular trustees (for example, in some jurisdictions professional regulatory authorities are required to deal with patient records abandoned by members that they regulate).
- 3) Government permits private records storage and processing companies with sound privacy practices to be considered for listing in the regulations as designated archives to provide for more options for transferring patient records.
- 4) The costs associated with transferring the records to the designated archive should remain the responsibility of the trustee who is leaving the field. A system should be developed to ensure that the funds required covering the costs of the designated archive services are paid by the trustee in some fashion. The Working Group is not unanimous on how this would be accomplished, but the discussion noted the following:
  - a. For trustees that are regulated by a professional regulatory authority, the professional regulatory authority could levy annual fees from the members and set up a fund to cover the costs associated with record storage where records are abandoned by their members. To facilitate member use of reasonable cost storage solutions, professional regulatory

authorities could co-operate and procure bulk arrangements with private storage companies to establish reduced fees from those that members might obtain individually for the service.

- b. Many other trustees are required to be licensed to carry on their health operations (personal care homes, health facilities, ambulance operators, etc.). The terms and conditions associated with licensing could require trustees to demonstrate that they have an arrangement or plan to deal with patient records on winding up operations and additional licensing fees could be assessed for the purposes of establishing a fund that the licensing body can access in the event records of an operator are abandoned.



## Summary and Conclusion

The Working Group notes that some of the analysis in this report centres on physician practice situations. This arose from the situations raised within the group for discussion which centered on physician-based situations. However, there are a number of other regulated professions with unique practice arrangements that may require further analysis to determine how HIPA applies to those arrangements. Accordingly, in relation to some of the recommendations, and in particular in relation to recommendation 4 regarding trustee practice arrangements, the Working Group suggests the Ministry of Health undertake further consultation with the health regulatory bodies to learn if there are additional situations of practice outside the definition of trustee in HIPA which are being engaged in.

The problem of abandoned records is not unique to Saskatchewan, and there is no single solution to the problem. The primary goal should be to insure that there are in place mechanisms to prevent records from becoming abandoned. These mechanisms require trustees to properly educate their staff in the handling of patient records, and for trustees to have a clear understanding of their responsibilities to the patient. Equally, it requires the legislation applicable to trustees' handling of these records to be complete and provide a system to address abandonment situations when they arise. The recommendations of the Working Group deal with prevention and systemic issues to attempt to prevent abandonment from occurring as well as providing for control and proper consequences when they do arise. The Working Group believes that the implementation of the foregoing recommendations will go a long distance to help to address the problems that were raised for its consideration and advice.

# Appendix A: Jurisdictional Scan

## British Columbia

### Freedom of Information and Protection of Privacy Act (FIPPA)

<p><b>Purpose of Legislation</b></p>	<p>2 (1) The purposes of the Act are to make public bodies more accountable to the public and to protect personal privacy by</p> <ul style="list-style-type: none"> <li>(a) giving the public a right of access to records,</li> <li>(b) giving individuals a right of access to, and a right to request correction of, personal information about themselves,</li> <li>(c) specifying limited exceptions to the rights of access,</li> <li>(d) preventing the unauthorized collection, use or disclosure of personal information by public bodies, and</li> <li>(e) providing for an independent review of decisions made under the Act.</li> </ul>
<p><b>Trustee / Custodian Definitions</b></p>	<p>The Act applies to all records in the custody or under the control of a public body.</p> <p>A public body includes provincial government public bodies, ministries, many government agencies, boards, commissions and Crown corporations. It also includes local public bodies such as municipalities, universities, colleges and school boards, hospitals, health boards, designated self-governing bodies of professional organizations such as the College of Physicians and Surgeons and the Law Society of British Columbia as examples and the “health information bank,” a ministry database within the meaning of the E-Health Act.</p> <p>The Act provides definitions for all bodies caught in the Schedules to the Act.</p> <p><b>“health care body”</b> means</p> <ul style="list-style-type: none"> <li>(a) a hospital as defined in section 1 of the <i>Hospital Act</i>,</li> <li>(b) a Provincial auxiliary hospital established under the <i>Hospital (Auxiliary) Act</i>,</li> <li>(c) a regional hospital district and a regional hospital district board under the <i>Hospital District Act</i>,</li> <li>(d) and (e) [Repealed 2008-28-147],</li> <li>(f) a Provincial mental health facility as defined in the <i>Mental Health Act</i>,</li> <li>(g) a regional health board designated under section 4 (1) of the <i>Health Authorities Act</i>, or</li> <li>(h) [Repealed 2002-61-17],</li> <li>(i) British Columbia Emergency Health Services, as described in section 2 (1) of the <i>Emergency Health Services Act</i>.</li> </ul> <p><b>“local government body”</b> means</p> <ul style="list-style-type: none"> <li>(a) a municipality,</li> <li>(b) [Repealed 2003-52-79],</li> <li>(c) a regional district,</li> <li>(d) an improvement district as defined in the <i>Local Government Act</i>,</li> <li>(e) a local area as defined in the <i>Local Services Act</i>,</li> <li>(f) a greater board as defined in the <i>Community Charter</i> or any incorporated board that provides similar services and is incorporated by letters patent,</li> <li>(g) a board of variance established under section 899 of the <i>Local Government Act</i> or section 572 of the <i>Vancouver Charter</i>,</li> <li>(h) the trust council, the executive committee, a local trust committee and the trust fund board, as these are defined in the <i>Islands Trust Act</i>,</li> <li>(i) the Okanagan Basin Water Board,</li> <li>(j) a water users’ community as defined in the <i>Water Act</i>,</li> <li>(k) the Okanagan-Kootenay Sterile Insect Release Board,</li> </ul>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Trustee / Custodian Definitions</b> <i>(continued)</i></p>	<p>(l) a municipal police board established under section 23 of the <i>Police Act</i>,  (m) a library board as defined in the <i>Library Act</i>,  (n) any board, committee, commission, panel, agency or corporation that is created or owned by a body referred to in paragraphs (a) to (m) and all the members or officers of which are appointed or chosen by or under the authority of that body,  (o) a board of trustees established under section 37 of the <i>Cremation, Interment and Funeral Services Act</i>,  (p) the South Coast British Columbia Transportation Authority, or  (q) the Park Board referred to in section 485 of the <i>Vancouver Charter</i>;</p> <p><b>“local public body”</b> means  (a) a local government body,  (b) a health care body,  (b.1) a social services body,  (c) an educational body, or  (d) a governing body of a profession or occupation, if the governing body is designated in, or added by regulation to, Schedule 3;</p> <p><b>“public body”</b> means  (a) a ministry of the government of British Columbia,  (b) an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2, or  (c) a local public body  but does not include  (d) the office of a person who is a member or officer of the Legislative Assembly, or  (e) the Court of Appeal, Supreme Court or Provincial Court.</p>
<p><b>How does Trustee Extend to Affiliates and Other Bodies?</b></p>	<p>The Act has definitions of associate and employees in relation to a public, and have specific provisions which make the duties in Part 3 (Privacy Protection) of the Act which apply to public bodies also apply to associates and employees of public bodies. Associates include officers and directors of public bodies, sub-contractors and service providers to a public body and related corporations to the public body. The specific definitions and provisions provide:</p> <p><b>“associate”</b> means, in relation to a service provider,  (a) an officer, director or partner of the service provider,  (b) an affiliate of the service provider,  (c) a subcontractor, or further sub-subcontractor, of the service provider or an affiliate of the service provider, or  (d) an employee, officer, director or partner of an affiliate referred to in paragraph (b) or of a subcontractor or further sub-subcontractor referred to in paragraph (c),  to or through whom access is made available to personal information that is  (e) subject to Division 2 (Use and Disclosure of Personal Information by Public Bodies) of Part 3, and  (f) held because of the service provider’s status as a service provider.</p> <p><b>“employee”</b>, in relation to a public body, includes  (a) a volunteer, and  (b) a service provider;</p> <p><b>31.1</b> The requirements and restrictions established by this Part also apply to  (a) the employees, officers and directors of a public body, and  (b) in the case of an employee that is a service provider, all employees and associates of the service provider.</p> <p><b>30.4</b> An employee, officer or director of a public body or an employee or associate of a service provider who has access, whether authorized or unauthorized, to personal information in the custody or control of a public body, must not disclose that information except as authorized under this Act.</p>
<p><b>Trustee/Custodian Responsibilities and Compliance Methods</b></p>	<p>Public bodies may only CUD PI as authorized In the Act.</p> <p>Investigations can be conducted on PI practises of public bodies by the Information and Privacy Commissioner and orders dealing with those practises and the maintenance and destruction of collected PI can be made.</p>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

Snooping – Unauthorized Viewing of PHI	*
<p><b>Mismanaged PHI and Abandoned Records</b></p>	<p>The Act has specific provisions allowing for recovery of PHI which has been improperly disclosed or is in the possession of a person not authorized to have the information. The provisions permit service of a notice on the party with the information and require the information to be returned or destroyed. Where not returned or destroyed, court orders can be obtained. The provisions provide:</p> <p><b>73.1</b> (1) If the head of a public body has reasonable grounds to believe that personal information in the custody or under the control of the public body is in the possession of a person or an entity not authorized by law to possess the information, the head of the public body may issue a written notice demanding that person or entity to do either of the following within 20 calendar days of receiving the notice:</p> <ul style="list-style-type: none"> <li>(a) return the information to the public body or, in the case of electronic records, securely destroy the information and confirm in writing the date and the means by which the information was securely destroyed;</li> <li>(b) respond in writing and declare why the person or entity considers that <ul style="list-style-type: none"> <li>(i) the information was not in the custody or under the control of the public body when the person or entity acquired possession of the information, or</li> <li>(ii) the person or entity is authorized by law to possess the information.</li> </ul> </li> </ul> <p>(2) The written notice referred to in subsection (1) must</p> <ul style="list-style-type: none"> <li>(a) identify, with reasonable specificity, the personal information claimed to be in the custody or under the control of the public body and in the possession of the person or entity not authorized by law to possess the information, and</li> <li>(b) state that the public body may undertake legal action to recover the personal information if the person or entity fails to respond in writing within the required time or does not adequately demonstrate that <ul style="list-style-type: none"> <li>(i) the information was not in the custody or under the control of the public body when the person or entity acquired possession of the information, or</li> <li>(ii) the person or entity is authorized by law to possess the information.</li> </ul> </li> </ul> <p><b>Court order for return of personal information</b></p> <p><b>73.2</b> (1) If a person or an entity that receives a written notice and demand from the public body under section 73.1 (1) fails to</p> <ul style="list-style-type: none"> <li>(a) return the described personal information or, in the case of electronic records, to securely destroy the information and confirm in writing the date and the means by which the information was securely destroyed,</li> <li>(b) respond to the notice and demand within the required time, or</li> <li>(c) adequately demonstrate that <ul style="list-style-type: none"> <li>(i) the personal information was not in the custody or under the control of the public body when the person or entity acquired possession of the information, or</li> <li>(ii) the person or entity is authorized by law to possess the personal information, the head of the public body may ask the Attorney General to petition the superior court in the jurisdiction in which the personal information is located for an order requiring the return of the personal information.</li> </ul> </li> </ul> <p>(2) If, after a hearing, the court determines that the personal information is in the possession of a person or an entity not authorized by law to possess the personal information and the public body is entitled to custody or control of the personal information, the court must order the personal information to be delivered to the head of the public body.</p> <p>(3) The court may issue any order necessary to protect the personal information from destruction, alteration or transfer by the person or entity in possession of the personal information and may order that the personal information be surrendered into the custody of the head of the public body until the court reaches a decision on the petition.</p>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Existing Offences/Penalties and Enforcement Approaches</b></p>	<p>Offences for breach of the Act exist</p> <p><b>74.1</b> (1) A person who contravenes section 30.4 (unauthorized disclosure) or 30.5 (notification of unauthorized disclosure) commits an offence.</p> <p>(2) A person who is a service provider or an employee or associate of a service provider commits an offence if the person does any of the following:</p> <ul style="list-style-type: none"> <li>(a) stores or allows access to personal information to which section 30.1 (location and access in Canada) applies contrary to that section;</li> <li>(b) contravenes section 30.2 (obligation to report foreign demand for disclosure);</li> <li>(c) contravenes section 30.3 (whistle-blower protection).</li> </ul> <p>(3) If an employee or associate of a service provider</p> <ul style="list-style-type: none"> <li>(a) stores or allows access to personal information to which section 30.1 (location and access in Canada) applies contrary to that section,</li> <li>(b) contravenes section 30.2 (obligation to report foreign demand for disclosure),</li> <li>(c) contravenes section 30.3 (whistle-blower protection),</li> <li>(d) contravenes section 30.4 (unauthorized disclosure), or</li> <li>(e) contravenes section 30.5 (notification of unauthorized disclosure),</li> </ul> <p>in relation to personal information that is held because of the service provider’s status as a service provider, the service provider commits an offence.</p> <p>(4) If a corporation commits an offence under this section, an officer, director or agent of the corporation who authorizes, permits or acquiesces in the commission of the offence also commits an offence, whether or not the corporation is prosecuted for the offence.</p> <p>(5) A person who commits an offence under this section is liable</p> <ul style="list-style-type: none"> <li>(a) in the case of an individual, other than an individual who is a service provider, to a fine of up to \$2,000,</li> <li>(b) in the case of a partnership that is or individual who is a service provider, to a fine of up to \$25,000, and</li> <li>(c) in the case of a corporation, to a fine of up to \$500,000.</li> </ul> <p>(6) The time limit for laying an information to commence a prosecution for an offence under this section is</p> <ul style="list-style-type: none"> <li>(a) one year after the date on which the act or omission that is alleged to constitute the offence occurred, or</li> <li>(b) if the minister responsible for this Act issues a certificate described in subsection (7), one year after the date on which the minister learned of the act or omission referred to in paragraph (a).</li> </ul>
<p><b>Designated Archives (Decisions Related to PHI Issues)</b></p>	<p>No similar concept to Designated Archives is present. Document Disposal Act applies to government public bodies-records handling.</p>
<p><b>Strict Liability and Identified Concerns</b></p>	<p>The Act provides specific provisions indicating that it is a defence for the person charged to prove that the person exercised due diligence to avoid the commission of the offence. (s. 74.1(8))</p>
<p><b>Educational Materials / Training</b></p>	<p>Office of the Chief Information Officer has information on website as does OIPC  <a href="http://www.cio.gov.bc.ca/cio/priv_leg/foipppa/leg_regs.page">http://www.cio.gov.bc.ca/cio/priv_leg/foipppa/leg_regs.page</a></p>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

Health Information Act

<p>Purpose of Legislation</p>	<p>2 The purposes of this Act are</p> <ul style="list-style-type: none"> <li>(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,</li> <li>(b) to enable health information to be shared and accessed, where appropriate, to provide health services and to manage the health system,</li> <li>(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,</li> <li>(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,</li> <li>(e) to provide individuals with a right to request correction or amendment of health information about themselves,</li> <li>(f) to establish strong and effective remedies for contraventions of this Act, and</li> <li>(g) to provide for independent reviews of decisions made by custodians under this Act and the resolution of complaints under this Act to protect the privacy of individuals with respect to their health information and to protect the confidentiality of that information, to enable health information to be shared and accessed.</li> </ul>
<p>Trustee / Custodian Definitions</p>	<p>Custodians collecting, using or disclosing health information pursuant to another enactment must comply with this Act:</p> <p><b>“custodian” means</b></p> <ul style="list-style-type: none"> <li>(i) the board of an approved hospital as defined in the <i>Hospitals Act</i> other than an approved hospital that is             <ul style="list-style-type: none"> <li>(A) owned and operated by a regional health authority established under the <i>Regional Health Authorities Act</i>,</li> <li>(B) repealed</li> </ul> </li> <li>(ii) the operator of a nursing home as defined in the <i>Nursing Homes Act</i> other than a nursing home that is owned and operated by a regional health authority established under the <i>Regional Health Authorities Act</i>;</li> <li>(ii.1) an ambulance operator as defined in the <i>Emergency Health Services Act</i>;</li> <li>(iii) a provincial health board established pursuant to regulations made under section 17(1)(a) of the <i>Regional Health Authorities Act</i>;</li> <li>(iv) a regional health authority established under the <i>Regional Health Authorities Act</i>;</li> <li>(v) a community health council as defined in the <i>Regional Health Authorities Act</i>;</li> <li>(vi) a subsidiary health corporation as defined in the <i>Regional Health Authorities Act</i>;</li> <li>(vii) repealed 2008 cH 5.3 s18;</li> <li>(viii) a board, council, committee, commission, panel or agency that is created by a custodian referred to in subclauses (i) to (vii), if all or a majority of its members are appointed by, or on behalf of, that custodian, but does not include a committee that has as its primary purpose the carrying out of quality assurance activities within the meaning of section 9 of the <i>Alberta Evidence Act</i>;</li> <li>(ix) a health services provider who is designated in the regulations as a custodian, or who is within a class of health services providers that is designated in the regulations for the purpose of this subclause;             <ul style="list-style-type: none"> <li>(ix.1) the Health Quality Council of Alberta;</li> </ul> </li> <li>(x) a licensed pharmacy as defined in the <i>Pharmacy and Drug Act</i>;</li> <li>(xi) repealed 2009 c25 s2;</li> <li>(xii) the Department;</li> <li>(xiii) the Minister;</li> <li>(xiv) an individual or board, council, committee, commission, panel, agency, corporation or other entity designated in the regulations as a custodian,</li> </ul>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Trustee / Custodian Definitions</b> (continued)</p>	<p><b>The following regulated health professionals are designated as custodians for (ix):</b></p> <ul style="list-style-type: none"> <li>(a) regulated members of the Alberta College and Association of Chiropractors;</li> <li>(b) regulated members of the Alberta College of Optometrists;</li> <li>(c) regulated members of the Alberta College of Pharmacists;</li> <li>(d) regulated members of the Alberta Dental Association and College;</li> <li>(e) regulated members of the College and Association of Registered Nurses of Alberta;</li> <li>(f) regulated members of the College of Alberta Denturists;</li> <li>(g) registered members of the College of Midwives of Alberta;</li> <li>(h) regulated members of the College of Opticians of Alberta;</li> <li>(i) regulated members of the College of Physicians and Surgeons of Alberta;</li> <li>(j) regulated members of the College of Podiatric Physicians of Alberta;</li> <li>(k) regulated members of the College of Registered Dental Hygienists of Alberta.</li> </ul>
<p><b>How does Trustee Extend to Affiliates and Other Bodies?</b></p>	<p>(a) “affiliate”, in relation to a custodian, means</p> <ul style="list-style-type: none"> <li>(i) an individual employed by the custodian,</li> <li>(ii) a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian,</li> <li>(iii) a health services provider who is exercising the right to admit and treat patients at a hospital as defined in the <i>Hospitals Act</i>,</li> <li>(iv) an information manager as defined in section 66(1), and</li> <li>(v) a person who is designated under the regulations to be an affiliate,</li> </ul> <p>but does not include</p> <ul style="list-style-type: none"> <li>(vi) an agent as defined in the <i>Health Insurance Premiums Act</i>, or</li> <li>(vii) a health information repository other than a health information repository that is designated in the regulations as an affiliate;</li> </ul> <p>Affiliates have their own specific duties under the legislation, which are similar to those of trustees, but do not have the same responsibility for maintaining the records. (eg: MDs practicing as employees are affiliates and only have the duties of affiliates in relation to Personal Health Information).</p> <p>S. 62(4) specifies that each affiliate of a custodian must comply with the Act and the policies and procedures set out by custodians. As well, S. 62(2) states any collection, use or disclosure by an affiliate of a custodian is considered a collection, use or disclosure by the custodian.</p>
<p><b>Trustee/Custodian Responsibilities and Compliance Methods</b></p>	<p>S. 62. this section requires each custodian to identify its affiliates who are responsible for ensuring that the Act, the regulations and the policies and procedures established or adopted by the custodian are complied with.</p> <p>Any collection, use or disclosure of health information by an affiliate of a custodian is considered to be a collection, use or disclosure by the custodian.</p> <p>Any disclosure of health information to an affiliate of a custodian is considered to be disclosure to the custodian . . . .</p>
<p><b>Snooping – Unauthorized Viewing of PHI</b></p>	<p>Custodians can only use personal health Information for purposes authorized by the Act.</p> <p>Section 28 precludes an affiliate from using personal health information in any manner that is not in accordance with the affiliate’s duties to the custodian.</p> <p>107 (2) No person shall knowingly</p> <ul style="list-style-type: none"> <li>(b) gain or attempt to gain access to health information in contravention of this Act</li> </ul>
<p><b>Mismanaged PHI and Abandoned Records</b></p>	<p>*</p>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Existing Offences/Penalties and Enforcement Approaches (Excerpt)</b></p>	<p>107(1) No custodian or affiliate of a custodian shall knowingly:</p> <ul style="list-style-type: none"> <li>(a) alter, falsify or conceal any record, or direct another person to do so, with the intent to evade a request for access to the record, or</li> <li>(b) destroy any record that is subject to this Act, or direct another person to do so, with the intent to evade a request for access to the record.</li> </ul> <p>(2) No person shall knowingly</p> <ul style="list-style-type: none"> <li>(a) collect, use, disclose or create health information in contravention of this Act,</li> <li>(b) gain or attempt to gain access to health information in contravention of this Act,</li> <li>(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,</li> <li>(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,</li> <li>(e) fail to comply with an order made by the Commissioner under section 80 or by an adjudicator under section 101, or</li> <li>(f) use individually identifying health information to market any service for a commercial purpose or to solicit money unless the individual who is the subject of the health information has specifically consented to its use for that purpose.</li> </ul> <p>(6) A person who contravenes this section, except subsection (5.1), is guilty of an offence and liable to a fine of not more than \$50,000.</p> <p>(6.1) Despite subsection (6), a person who uses prescribed health information in contravention of section 56.4 is guilty of an offence and liable to a fine of not more than \$100,000.</p> <p>A prosecution under the Act may be commenced within 2 years after the commission of the alleged offence.</p> <p>No particular offences apply to abandoned records.</p>
<p><b>Designated Archives (Decisions Related to PHI Issues)</b></p>	<p>The Act provides for Health Information Repositories to which custodians can disclose personal health information, but no functions or duties are specified.</p>
<p><b>Strict Liability and Identified Concerns</b></p>	<p>*</p>
<p><b>Educational Materials / Training</b></p>	<p>AHS Traiing material available on their website at <a href="http://www.albertahealthservices.ca/3962.asp">www.albertahealthservices.ca/3962.asp</a></p> <p>S. 63 prescribes that custodian must implement procedure to facilitate compliance with the Act – these procedures include training.</p>

## Saskatchewan

### **The Health Information Protection Act (HIPA)**

<p><b>Purpose of Legislation</b></p>	<p>No Specific Purpose clause in legislation.</p> <p>Legislation governs the collection, use and disclosure of personal health Information by Trustees, provides for specific rights of individuals in relation to personal health information and gives individuals rights of access to their own personal health information.</p>
--------------------------------------	---

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.



<p><b>Trustee / Custodian Definitions</b></p>	<p>2 In this Act:</p> <p>(e) <b>“designated archive”</b> means an archive designated in the regulations for the purposes of section 22;</p> <p>(t) <b>“trustee”</b> means any of the following that have custody or control of personal health information:</p> <ul style="list-style-type: none"> <li>(i) a government institution;</li> <li>(ii) a regional health authority or a health care organization;</li> <li>(iii) <b>Repealed.</b> 2002, c.R-8.2, s.77.</li> <li>(iv) a licensee as defined in <i>The Personal Care Homes Act</i>;</li> <li>(v) a person who operates a facility as defined in <i>The Mental Health Services Act</i>;</li> <li>(vi) a licensee as defined in <i>The Health Facilities Licensing Act</i>;</li> <li>(vii) an operator as defined in <i>The Ambulance Act</i>;</li> <li>(viii) a licensee as defined in <i>The Medical Laboratory Licensing Act, 1994</i>;</li> <li>(ix) a proprietor as defined in <i>The Pharmacy Act, 1996</i>;</li> <li>(x) a community clinic: <ul style="list-style-type: none"> <li>(A) as defined in section 263 of <i>The Co-operatives Act, 1996</i>;</li> <li>(B) within the meaning of section 9 of <i>The Mutual Medical and Hospital Benefit Associations Act</i>; or</li> <li>(C) incorporated or continued pursuant to <i>The Non-profit Corporations Act, 1995</i>;</li> </ul> </li> <li>(xi) the Saskatchewan Cancer Foundation;</li> <li>(xii) a person, other than an employee of a trustee, who is: <ul style="list-style-type: none"> <li>(A) a health professional licensed or registered pursuant to an Act for which the minister is responsible; or</li> <li>(B) a member of a class of persons designated as health professionals in the regulations;</li> </ul> </li> <li>(xiii) a health professional body that regulates members of a health profession pursuant to an Act;</li> <li>(xiv) a person, other than an employee of a trustee, who or body that provides a health service pursuant to an agreement with another trustee;</li> <li>(xv) any other prescribed person, body or class of persons or bodies;</li> </ul> <p>* In situations where a health professional is employed by a trustee (for example, a nurse employed by a regional health authority), the employer is considered the trustee.</p>
<p><b>How does Trustee Extend to Affiliates and Other Bodies?</b></p>	<p>No similar concept to Alberta’s affiliate definition.</p> <p>Statutory duties are placed on Trustees. Trustees are responsible to have in place policies and procedures governing their employees’ actions.</p>
<p><b>Trustee/Custodian Responsibilities and Compliance Methods</b></p>	<p>Specific duties under the legislation made applicable to Trustees in regard to use, collection and disclosure and destruction of personal health information in Part III of Act. (sections 16 - 22). Specific duty for protection of personal health Information in section 16</p> <p>S. 16 Subject to the regulations, a trustee that has custody or control of PHI must establish policies and procedures to maintain administrative, technical and physical safeguards that will:</p> <ul style="list-style-type: none"> <li>(a) protect the integrity, accuracy and confidentiality of the information;</li> <li>(b) protect against any reasonably anticipated: <ul style="list-style-type: none"> <li>(i) threat or hazard to the security or integrity of the information;</li> <li>(ii) loss of the information; or</li> <li>(iii) unauthorized access to or use, disclosure or modification of the information; and</li> </ul> </li> <li>(c) otherwise ensure compliance with this Act by its employees.</li> </ul>
<p><b>Snooping – Unauthorized Viewing of PHI</b></p>	<p>No specific offence provision. Provisions requiring policies to be in place to restrict employee access to only those who need to know information.</p> <p>23((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.</p>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Mismanaged PHI and Abandoned Records</b></p>	<p>Section 22 requires exiting trustees to maintain control of records until transferred to a new trustee or designated archive.</p> <p><b>22(1)</b> Where a trustee ceases to be a trustee with respect to any records containing personal health information, the duties imposed by this Act on a trustee with respect to personal health information in the custody or control of the trustee continue to apply to the former trustee until the former trustee transfers custody and control of the personal health information to another trustee or to an information management service provider that is a designated archive.</p> <p>(2) Where a former trustee fails to carry out the duties continued pursuant to subsection (1), the minister may appoint a person or body to act in place of the former trustee until custody and control of the personal health information is transferred to another trustee or to an information management service provider that is a designated archive.</p>
<p><b>Existing Offences/Penalties and Enforcement Approaches</b></p>	<p><b>64(1)</b> No person shall:</p> <ul style="list-style-type: none"> <li>(a) knowingly contravene any provision of this Act or the regulations;</li> <li>(b) without lawful justification or excuse, wilfully obstruct, hinder or resist the commissioner or any other person in the exercise of the powers, performance of the duties or the carrying out of the functions of the commissioner or other person pursuant to this Act;</li> <li>(c) without lawful justification or excuse, refuse or wilfully fail to comply with any lawful requirement of the commissioner or any other person pursuant to this Act;</li> <li>(d) wilfully make any false statement to, or mislead or attempt to mislead, the commissioner or any other person in the exercise of the powers, performance of the duties or carrying out of the functions of the commissioner or other person pursuant to this Act;</li> <li>(e) wilfully destroy any record that is governed by this Act with the intent to evade a request for access to the record; or</li> <li>(f) obtain another person’s personal health information by falsely representing that he or she is entitled to the information.</li> </ul> <p>(2) Every person who contravenes subsection (1) is guilty of an offence and is liable on summary conviction:</p> <ul style="list-style-type: none"> <li>(a) in the case of an individual, to a fine of not more than \$50,000, to imprisonment for not more than one year or to both; and</li> <li>(b) in the case of a corporation, to a fine of not more than \$500,000.</li> </ul> <p>(3) Every director, officer or agent of a corporation who directed, authorized, assented to, acquiesced in or participated in an act or omission of the corporation that would constitute an offence by the corporation is guilty of that 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 corporation has been prosecuted or convicted.</p> <p>(4) No prosecution shall be commenced pursuant to this section except with the express consent of the Attorney General for Saskatchewan.</p> <p>(5) No prosecution shall be commenced pursuant to this section after the expiration of two years after the date of the discovery of the alleged offence.</p>
<p><b>Designated Archives (Decisions Related to PHI Issues)</b></p>	<p>Trustees can transfer records to designated archives.</p> <p>The following are designated archives:</p> <ul style="list-style-type: none"> <li>(a) affiliates;</li> <li>(b) the Ministry of Health;</li> <li>(c) health professional bodies that regulate members of a health profession pursuant to an Act;</li> <li>(d) regional health authorities;</li> <li>(e) Saskatchewan Archives Board;</li> <li>(f) Ehealth Saskatchewan;</li> <li>(g) University of Regina Archives;</li> <li>(h) University of Saskatchewan Archives.</li> </ul> <p>Nothing requires a designated archive to accept PHI records from a trustee.</p>

\*Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

Strict Liability and Identified Concerns	*
Educational Materials / Training	Online brochure; <a href="http://www.health.gov.sk.ca/hipa-brochure">www.health.gov.sk.ca/hipa-brochure</a>

## Manitoba

### ***The Personal Health Information Act (PHIA)***

<b>Purpose of Legislation</b>	<p>The purposes of the Act are</p> <ul style="list-style-type: none"> <li>(a) to provide individuals with a right to examine and receive a copy of PHI about themselves maintained by a trustee, subject to the limited and specific exceptions set out in the Act;</li> <li>(b) to provide individuals with a right to request corrections to PHI about themselves maintained by a trustee;</li> <li>(c) to establish rules governing the collection, use, disclosure, retention and destruction of PHI in a manner that recognizes <ul style="list-style-type: none"> <li>(i) the right of individuals to privacy of their personal health Information, and</li> <li>(ii) the need for health professionals to collect, use and disclose personal health information in order to provide health care to individuals;</li> </ul> </li> <li>(d) to control the collection, use and disclosure of an individual's PHIN; and</li> <li>(e) to provide for an independent review of the decisions of trustees under this Act.</li> </ul>
<b>Trustee / Custodian Definitions</b>	<p>"Trustee" means a health professional, health care facility, public body, or health services agency that collects or maintains personal health information.</p> <p>"maintain" is defined to mean to have "custody or control" of the information.</p> <p>"Health care facility" means:</p> <ul style="list-style-type: none"> <li>(a) a hospital,</li> <li>(b) a personal care home,</li> <li>(c) a psychiatric facility,</li> <li>(d) a medical clinic,</li> <li>(e) a laboratory,</li> <li>(f) CancerCare Manitoba, and</li> <li>(g) a community health centre or other facility in which health care is provided and that is designated in the regulations.</li> </ul> <p>"Health professional" means a person who is licensed or registered to provide health care under an Act of the Legislature or who is a member of a class of persons designated as health professionals in the regulations.</p> <p>"Health services agency" means an organization that provides health care such as community or home-based health care pursuant to an agreement with another trustee.</p> <p>"public body" means a public body as defined in The Freedom of Information and Protection of Privacy Act, and for the purpose of this definition, the definitions of "department", "educational body", "government agency", "health care body", "local government body" and "local public body" in that Act apply.</p>
<b>How does Trustee Extend to Affiliates and Other Bodies?</b>	<p>No similar concept to affiliate definition in Alberta - Act's duties apply to Trustees.</p> <p>61(2) Any action done by, or information disclosed to, a person employed by or in the service of a trustee in the performance of that person's duties is deemed to have been done by, or disclosed to, the trustee for the purposes of this Act.</p> <p>Under other legislation corporations are precluded from carrying on the practice of a Regulated Health Profession unless the corporation is authorized to do so in the regulations to the Act. That corporation could then be specifically known and dealt with as a Trustee under Manitoba's <i>Personal Health Information Act</i>.</p>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Trustee/Custodian Responsibilities and Compliance Methods</b></p>	<p>Trustees have two main obligations:</p> <ol style="list-style-type: none"> <li>1) to provide individuals access to their own PHI that the trustee maintains, and</li> <li>2) to protect the privacy of that PHI and to collect, use and disclose only in accordance with the Act's authorities.</li> </ol>
<p><b>Snooping – Unauthorized Viewing of PHI</b></p>	<p>Manitoba recently enacted specific offence provisions dealing with unauthorized access to personal health information</p> <p>63(2) Despite subsection 61(2), a person who is an employee, officer or agent of a trustee, information manager or health research organization and who, without the authorization of the trustee, information manager or health research organization, wilfully</p> <ol style="list-style-type: none"> <li>(a) discloses personal health information in circumstances where the trustee, information manager or health research organization would not be permitted to disclose the information under this Act; or</li> <li>(b) uses, gains access to or attempts to gain access to another person's personal health information;</li> </ol> <p>is guilty of an offence.</p>
<p><b>Mismanaged PHI and Abandoned Records</b></p>	<p>No specific provisions in legislation addressing abandoned records.</p> <p>Ombudsman investigates complaints.</p> <p>Physicians planning to leave clinical practice must notify their regulatory body of the name, address, and telephone number of the new custodian of the medical records. Manitoba advises if records are at risk of being abandoned the regulator of physician practise is responsible for securing and protecting the records. The regulator can appoint a member as a custodian or apply to the court for a custodian, but is required to monitor the custodian. After 30 days the regulator is deemed to be the custodian.</p>
<p><b>Existing Offences/Penalties and Enforcement Approaches (Excerpt)</b></p>	<p>63(1) Any person who</p> <ol style="list-style-type: none"> <li>(a) wilfully makes a false statement to, or misleads or attempts to mislead, the Ombudsman or another person in the performance of the duties and powers of the Ombudsman;</li> <li>(b) wilfully obstructs the Ombudsman, or any person acting for or under the direction of the Ombudsman, in any manner;</li> <li>(c) wilfully destroys or erases personal health information with the intent to evade an individual's request to examine or copy the information;</li> <li>(d) obtains another person's personal health information by falsely representing that he or she is entitled to the information;</li> <li>(e) requires production of or collects or uses another person's PHIN contrary to section 26;</li> </ol> <p>or</p> <ol style="list-style-type: none"> <li>(f) knowingly falsifies another person's personal health information;</li> </ol> <p>is guilty of an offence.</p> <p>63(2) Despite subsection 61(2), a person who is an employee, officer or agent of a trustee, information manager or health research organization and who, without the authorization of the trustee, information manager or health research organization, wilfully</p> <ol style="list-style-type: none"> <li>(a) discloses personal health information in circumstances where the trustee, information manager or health research organization would not be permitted to disclose the information under this Act; or</li> <li>(b) uses, gains access to or attempts to gain access to another person's personal health information;</li> </ol> <p>is guilty of an offence.</p> <p>63(3) A trustee, information manager or health research organization who</p> <ol style="list-style-type: none"> <li>(a) collects, uses, sells or discloses personal health information contrary to this Act;</li> <li>(b) fails to protect personal health information in a secure manner as required by this Act; or</li> <li>(c) discloses personal health information contrary to this Act with the intent to obtain a monetary or other material benefit or to confer such a benefit on a trustee or other person;</li> </ol> <p>is guilty of an offence.</p>

\*Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<b>Existing Offences/Penalties and Enforcement Approaches (Excerpt) (continued)</b>	63(5) When a contravention of this Act continues for more than one day, the person is guilty of a separate offence for each day the contravention continues. 63(6) A prosecution under this Act may be commenced not later than two years after the commission of the alleged offence.
<b>Designated Archives (Decisions Related to PHI Issues)</b>	*
<b>Strict Liability and Identified Concerns</b>	Due diligence defence is available for certain types of offences. 63(4) No trustee, information manager or health research organization shall be found to have contravened clause (3)(a) or (b) if the trustee, information manager or health research organization can establish that he or she took all reasonable steps to prevent the contravention.
<b>Educational Materials / Training</b>	Manitoba Health provides PHIA training free of charge to any organization in the province. Trustees are responsible for their own ongoing training and awareness programs. Looking at putting together a PHIA awareness program package to boost start these programs in trustee organizations. <a href="http://www.gov.mb.ca/health/phia/docs/general_june2013.pdf">www.gov.mb.ca/health/phia/docs/general_june2013.pdf</a>

## Ontario

### ***Personal Health Information Protection Act, 2004***

<b>Purpose of Legislation</b>	<p>1. The purposes of the Act are,</p> <ul style="list-style-type: none"> <li>(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;</li> <li>(b) to provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions set out in the Act;</li> <li>(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 the Act;</li> <li>(d) to provide for independent review and resolution of complaints with respect to personal health information; and</li> <li>(e) to provide effective remedies for contraventions of the Act.</li> </ul>
-------------------------------	--

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Trustee / Custodian Definitions</b></p>	<p>Act defines custodians and includes system for determining responsibilities to assign single custodian at facilities or multiple facilities.</p> <p>“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:</p> <ol style="list-style-type: none"> <li>1. A health care practitioner or a person who operates a group practice of health care practitioners.</li> <li>2. A service provider within the meaning of the <i>Home Care and Community Services Act, 1994</i> who provides a community service to which that Act applies.</li> <li>3. A community care access corporation within the meaning of the <i>Community Care Access Corporations Act, 2001</i>.</li> <li>4. A person who operates one of the following facilities, programs or services: <ol style="list-style-type: none"> <li>i. A hospital within the meaning of the <i>Public Hospitals Act</i>, a private hospital within the meaning of the <i>Private Hospitals Act</i>, a psychiatric facility within the meaning of the <i>Mental Health Act</i> or an independent health facility within the meaning of the <i>Independent Health Facilities Act</i>.</li> <li>ii. A long-term care home within the meaning of the <i>Long-Term Care Homes Act, 2007</i>, a placement co-ordinator described in subsection 40 (1) of that Act, or a care home within the meaning of the <i>Residential Tenancies Act, 2006</i>.</li> <li>ii.1 a retirement home within the meaning of the <i>Retirement Homes Act, 2010</i>.</li> <li>iii. A pharmacy within the meaning of Part VI of the <i>Drug and Pharmacies Regulation Act</i>.</li> <li>iv. A laboratory or a specimen collection centre as defined in section 5 of the <i>Laboratory and Specimen Collection Centre Licensing Act</i>.</li> <li>v. An ambulance service within the meaning of the <i>Ambulance Act</i>.</li> <li>vi. A home for special care within the meaning of the <i>Homes for Special Care Act</i>.</li> <li>vii. A centre, program or service for community health or mental health whose primary purpose is the provision of health care.</li> </ol> </li> <li>5. An evaluator within the meaning of the <i>Health Care Consent Act, 1996</i> or an assessor within the meaning of the <i>Substitute Decisions Act, 1992</i>.</li> <li>6. A medical officer of health of a board of health within the meaning of the <i>Health Protection and Promotion Act</i>.</li> <li>7. The Minister, together with the Ministry of the Minister, if the context so requires.</li> <li>8. Any other person prescribed as a health information custodian if the person has custody or control of personal health information as a result of or in connection with performing prescribed powers, duties or work or any prescribed class of such persons.</li> </ol> <p>“health care practitioner” means,</p> <ol style="list-style-type: none"> <li>(a) a person who is a member within the meaning of the <i>Regulated Health Professions Act, 1991</i> and who provides health care,</li> <li>(b) a person who is registered as a drugless practitioner under the <i>Drugless Practitioners Act</i> and who provides health care,</li> <li>(c) a person who is a member of the Ontario College of Social Workers and Social Service Workers and who provides health care, or</li> <li>(d) any other person whose primary function is to provide health care for payment.</li> </ol> <p>Definitions exclude an aboriginal healer who provides traditional healing services to aboriginal persons or members of an aboriginal community; an aboriginal midwife who provides traditional midwifery services to aboriginal persons or members of an aboriginal community; and a person who treats another person solely by prayer or spiritual means in accordance with the tenets of the religion of the person giving the treatment.</p>
<p><b>How does Trustee Extend to Affiliates and Other Bodies?</b></p>	<p>Act has provisions similar to Alberta’s affiliate provisions creating rules for employees and contractors of health information custodians called “agents.”</p> <p>“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 PHI 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.</p>

\*Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Trustee/Custodian Responsibilities and Compliance Methods</b></p>	<p>Custodians are responsible for complying with the Act’s requirements for the PHI in their custody and control. Custodians are also responsible for safeguarding and protecting this PHI and must have privacy policies and procedures in place.</p> <p>PHIPA sections 10 to 17 lay out a custodian’s responsibilities to protect personal health information in its custody.</p> <p>Custodians, such as physicians, must also comply with data retention schedules provided by their respective professional colleges and/or associations. PHIPA does not have provision for data retention schedules.</p> <p>If a health information custodian dies, the following person shall be deemed to be the health information custodian with respect to records of PHI held by the deceased custodian until custody and control of the records, where applicable, passes to another person who is legally authorized to hold the records:</p> <ol style="list-style-type: none"> <li>1. The estate trustee of the deceased custodian.</li> <li>2. The person who has assumed responsibility for the administration of the deceased custodian’s estate, if the estate does not have an estate trustee.</li> </ol>
<p><b>Snooping – Unauthorized Viewing of PHI</b></p>	<p>No specific offence provision like Manitoba dealing with employees.</p>
<p><b>Mismanaged PHI and Abandoned Records</b></p>	<p>No specific provisions dealing with taking control of abandoned records. Custodians are also responsible for the safe-keeping of records in their custody until such a time that they are transferred to another custodian. For instance, If a physician retires, they must inform their patients on how they can access their record.</p> <p>Provisions dealing with requirements for protection of records and notification for breach exist as well as for notification of contravention to Commissioner.</p> <p>12. (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that PHI in the custodian’s custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.</p> <p>(2) Subject to subsection (3) and subject to the exceptions and additional requirements, if any, that are prescribed, a health information custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons.</p> <p>56. (1) A person who has reasonable grounds to believe that another person has contravened or is about to contravene a provision of this Act or its regulations may make a complaint to the Commissioner.</p>
<p><b>Existing Offences/Penalties and Enforcement Approaches</b></p>	<p>If a health information custodian uses or discloses PHI about an individual, without the individual’s consent, in a manner that is outside the scope of the custodian’s description of its information practices under clause (1) (a), the custodian shall inform the individual of the uses and disclosures at the first reasonable opportunity and make a note of the uses and disclosures. The custodian is to keep the note as part of the records of PHI about the individual that it has in its custody or under its control or in a form that is linked to those records.</p> <p><b>72.</b> (1) A person is guilty of an offence if the person,</p> <ol style="list-style-type: none"> <li>(a) wilfully collects, uses or discloses personal health information in contravention of this Act or its regulations;</li> <li>(b) makes a request under this Act, under false pretences, for access to or correction of a record of personal health information;</li> <li>(c) in connection with the collection, use or disclosure of personal health information or access to a record of personal health information, makes an assertion, knowing that it is untrue, to the effect that the person, <ol style="list-style-type: none"> <li>(i) is a person who is entitled to consent to the collection, use or disclosure of personal health information about another individual,</li> <li>(ii) meets the requirement of clauses 26 (2) (b) and (c),</li> <li>(iii) holds the beliefs described in subsection 26 (5), or</li> <li>(iv) is a person entitled to access a record of personal health information under section 52;</li> </ol> </li> </ol>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Existing Offences/Penalties and Enforcement Approaches</b> (continued)</p>	<p>(d) disposes of a record of personal health information in the custody or under the control of the custodian with an intent to evade a request for access to the record that the custodian has received under subsection 53 (1);</p> <p>(e) wilfully disposes of a record of personal health information in contravention of section 13;</p> <p>(f) contravenes subsection 34 (2), (3) or (4) or clause 47 (15) (a), (e) or (f);</p> <p>(g) wilfully obstructs the Commissioner or a person known to be acting under the authority of the Commissioner in the performance of his or her functions under this Act;</p> <p>(h) wilfully makes a false statement to mislead or attempt to mislead the Commissioner or a person known to be acting under the authority of the Commissioner in the performance of his or her functions under this Act;</p> <p>(i) wilfully fails to comply with an order made by the Commissioner or a person known to be acting under the authority of the Commissioner under this Act; or</p> <p>(j) contravenes section 70.</p> <p>(2) A person who is guilty of an offence under subsection (1) is liable, on conviction,</p> <p>(a) if the person is a natural person, to a fine of not more than \$50,000; and</p> <p>(b) if the person is not a natural person, to a fine of not more than \$250,000.</p>
<p><b>Designated Archives (Decisions Related to PHI Issues)</b></p>	<p>Prescribed registries are Ontario's equivalent of Saskatchewan's designated archives. Registries must have privacy policies and procedures in place which must be reviewed and approved every three years by the Information Privacy Commissioner.</p>
<p><b>Strict Liability and Identified Concerns</b></p>	<p>*</p>
<p><b>Educational Materials / Training</b></p>	<p>Educational materials pertaining to privacy and the protection of PHI are developed by the Information Privacy Commissioner. These can be found at: <a href="http://www.ipc.on.ca/english/resources/">www.ipc.on.ca/english/resources/</a></p>

## New Brunswick

### Personal Health Information Privacy and Access Act (PHIPAA)

<p><b>Purpose of Legislation</b></p>	<p>The purposes of the Act are</p> <p>(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 the Act,</p> <p>(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 the Act,</p> <p>(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,</p> <p>(d) to facilitate the effective provision of care and planning and management of the health care system,</p> <p>(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,</p> <p>(f) to establish mechanisms to safeguard the security and integrity of personal health information by those persons having custody or control of that information,</p> <p>(g) to provide for an independent review and resolution of complaints made in respect to personal health information, and</p> <p>(h) to provide effective remedies for contraventions of the Act.</p>
--------------------------------------	--

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.



<p><b>Trustee / Custodian Definitions</b></p>	<p>custodian - means an individual or organization that collects, maintains or uses personal health information for the purpose of providing or assisting in the provision of health care or treatment or the planning and management of the health care system or delivering a government program or service and includes</p> <ul style="list-style-type: none"> <li>(a) public bodies,</li> <li>(b) health care providers,</li> <li>(c) the Minister,</li> <li>(d) the following organizations or agencies: <ul style="list-style-type: none"> <li>(i) Ambulance New Brunswick Inc.,</li> <li>(ii) the New Brunswick Health Council,</li> <li>(iii) Facilicorp NB Ltd.,</li> <li>(iv) regional health authorities,</li> <li>(v) the Workplace Health, Safety and Compensation Commission, and</li> <li>(vi) the Canadian Blood Services,</li> </ul> </li> <li>(e) information managers,</li> <li>(e.1) research data centres,</li> <li>(f) researchers conducting a research project approved in accordance with this Act,</li> <li>(g) health care facilities,</li> <li>(h) a laboratory or a specimen collection centre,</li> <li>(i) nursing homes and operators as those terms are defined in the Nursing Homes Act, and</li> <li>(j) a person designated in the regulations as a custodian.</li> </ul>
<p><b>How does Trustee Extend to Affiliates and Other Bodies?</b></p>	<p>The Act includes a definition for “agent” to extend the application of the Act’s rules to third parties that are collecting, using or disclosing PHI on a custodian’s behalf:</p> <p>agent - in relation to a custodian, means an individual or organization that acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian and not for the agent’s own purposes, whether or not employed by the custodian or being remunerated.</p>
<p><b>Trustee/Custodian Responsibilities and Compliance Methods</b></p>	<p>Custodians (as defined in the Act) are responsible for collecting, maintaining or using PHI for the purposes of providing or assisting in the provision of health care, treatment, planning and management of the health-care system, or delivering a government program/service.</p> <p>Custodians must establish and comply with a written policy for the retention, archival storage, access, and secure destruction of PHI that meets the requirements.</p> <p>Act restricts amount of PHI to be disclosed:</p> <p><b>35(2)</b> Every disclosure by a custodian of personal health information shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is disclosed.</p> <p><b>35(3)</b> A custodian shall limit the disclosure of personal health information it maintains to those employees and agents of the custodian who need to know the information to carry out the purpose for which the information was collected or received or to carry out a purpose authorized under section 37.</p> <p>NB expects that physicians will advise the individual of the location of the records after their practice closes – custodian obligations remain until this has been successfully transferred to another custodian under section 54.</p>
<p><b>Snooping – Unauthorized Viewing of PHI</b></p>	<p>*</p>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Mismanaged PHI and Abandoned Records</b></p>	<p>No specific provisions on abandoned records but the Act provides for successorship obligations:</p> <p>38 (2) For the purpose of paragraph (1)(j), a custodian who transfers a record of PHI to its successor shall make reasonable efforts to give notice to the individual to whom the information relates before the transfer or, if this is not possible, as soon as possible after the transfer, that it has ceased to be a custodian of the information and identifies its successor.</p> <p>54(1) Subject to this section, a custodian does not cease to be a custodian with respect to a record of PHI until complete custody and control of the record passes to another person who is legally authorized to hold the record.</p> <p>54(3) If a custodian who is an individual dies, the duties and powers of a custodian under this Act shall be performed by the personal representative of the deceased... until custody and control of the record of PHI passes to another person who is legally authorized to hold the record.</p> <p>NB advises that its physician regulatory body has the authority by court order to seize abandoned records or records at risk for being abandoned.</p>
<p><b>Existing Offences/Penalties and Enforcement Approaches</b></p>	<p>Specific employee offence provisions exist in section 76(2).</p> <p><b>76(1)</b>No person shall</p> <ul style="list-style-type: none"> <li>(a) collect, use or disclose personal health information in wilful contravention of this Act,</li> <li>(b) attempt to gain or gain access to personal health information in wilful contravention of this Act,</li> <li>(c) knowingly make a false or misleading statement to the Commissioner or another person in the performance of the duties or the exercise of the powers of the Commissioner or the other person under this Act or knowingly mislead or attempt to mislead the Commissioner or the other person,</li> <li>(d) obstruct the Commissioner or another person in performing duties or exercising powers under this Act,</li> <li>(e) destroy a record or erase information in a record that is subject to this Act, or direct another person to do so, with the intent to evade a request to examine or copy the record,</li> <li>(f) alter, falsify, conceal or destroy any record or part of any record, or direct another person to do so, with an intent to evade a request to examine or copy the record, or</li> <li>(g) wilfully fail to comply with an investigation of the Commissioner.</li> </ul> <p><b>76(2)</b> A person who is an employee of a custodian or information manager who, without the authorization of the custodian or information manager, discloses personal health information in wilful contravention of this Act in circumstances where the custodian or information manager would not be permitted to disclose the information under this Act, commits an offence.</p> <p><b>76(3)</b> A custodian or information manager commits an offence if the custodian or information manager</p> <ul style="list-style-type: none"> <li>(a) collects, uses, sells or discloses personal health information contrary to this Act,</li> <li>(b) fails to protect personal health information in a secure manner as required by this Act,</li> <li>(c) discloses personal health information contrary to this Act with the intent of obtaining a monetary or other material benefit or to confer a benefit on a custodian or other person, or</li> <li>(d) takes any adverse employment action against an employee because the employee has complied with a request or requirement to produce a record or provide information or evidence to the Commissioner, or a person acting for or under the direction of the Commissioner, under this Act.</li> </ul> <p>See <i>The Provincial Offences Procedures Act</i> outlines penalties/fines.</p>
<p><b>Designated Archives (Decisions Related to PHI Issues)</b></p>	<p>No similar provisions to Saskatchewan's Designated Archives.</p>
<p><b>Strict Liability and Identified Concerns</b></p>	<p>Yes - Due diligence defence.</p> <p><b>76(4)</b> No custodian or information manager shall be found to have contravened paragraph (3) (a) or (b) if the custodian or information manager can establish that he or she took all reasonable steps to prevent the contravention.</p>
<p><b>Educational Materials / Training</b></p>	<p>*</p>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

# Newfoundland/Labrador

## Personal Health Information Act

<p><b>Purpose of Legislation</b></p>	<p><b>3.</b> The purposes of the Act are</p> <ul style="list-style-type: none"> <li>(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;</li> <li>(b) to provide individuals with a right of access to personal health information about themselves, subject to limited and specific exceptions set out in the Act;</li> <li>(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 the Act;</li> <li>(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;</li> <li>(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</li> <li>(f) to establish measures to promote the compliance with the Act by persons having the custody or control of personal health information.</li> </ul>
<p><b>Trustee / Custodian Definitions</b></p>	<p><b>4.</b> (1) In this Act, “custodian” means a person described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with the performance of the person’s powers or duties or the work described in that paragraph:</p> <ul style="list-style-type: none"> <li>(a) an authority;</li> <li>(b) a board, council, committee, commission, corporation or agency established by an authority;</li> <li>(c) a department created under the <i>Executive Council Act</i>, or a branch of the executive government of the province, when engaged in a function related to the delivery or administration of health care in the province;</li> <li>(d) the minister, where the context so requires;</li> <li>(e) a health care professional, when providing health care to an individual or performing a function necessarily related to the provision of health care to an individual;</li> <li>(f) a health care provider;</li> <li>(g) a person who operates             <ul style="list-style-type: none"> <li>(i) a health care facility,</li> <li>(ii) a licensed pharmacy as defined in the <i>Pharmacy Act, 2012</i>,</li> <li>(iii) an ambulance service, or</li> <li>(iv) a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health care provider;</li> </ul> </li> <li>(h) the Provincial Public Health Laboratory;</li> <li>(i) the Centre for Health Information;</li> <li>(j) with respect to Memorial University of Newfoundland, the Faculty of Medicine, the School of Nursing, the School of Pharmacy and the School of Human Kinetics and Recreation;</li> <li>(k) the Centre for Nursing Studies;</li> <li>(l) the Western Regional School of Nursing;</li> <li>(m) a person who, as a result of the bankruptcy or insolvency of a custodian, obtains complete custody or control of a record of personal health information, held by the custodian;</li> <li>(n) a rights advisor under the <i>Mental Health Care and Treatment Act</i>;</li> <li>(o) the Workplace Health, Safety and Compensation Commission; and</li> <li>(p) a person designated as a custodian in the regulations.</li> </ul> <p>Employees of custodians are specifically identified as not being custodians nor are regulatory bodies which are responsible for regulation of health professions.</p>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>How does Trustee Extend to Affiliates and Other Bodies?</b></p>	<p>Act extends to third party agents of custodians:</p> <p>2. (1) In this Act (a) "agent", in relation to a custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of PHI for the purposes of the custodian, and not the agent's purposes, whether or not the agent has the authority to bind the custodian, is paid by the custodian or is being remunerated by the custodian;</p> <p>Custodians are required to establish policies governing use, collection, disclosure and protection of PHI. Employees/agents and health care professionals providing services in a facility operated by a custodian are required to follow those policies:</p> <p>14(1) A custodian shall ensure that</p> <ul style="list-style-type: none"> <li>(a) its employees, agents, contractors and volunteers; and</li> <li>(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,</li> </ul> <p>take an oath or affirmation of confidentiality.</p> <p>(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</p> <ul style="list-style-type: none"> <li>(a) this Act and the regulations; and</li> <li>(b) the information policies and procedures referred to in subsection 13(1).</li> </ul> <p>(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.</p>
<p><b>Trustee/Custodian Responsibilities and Compliance Methods</b></p>	<p>Act provides rules for transfer of records when custodians exit practice. Custodian remains in control of records until transferred to another custodian.</p> <p>4(3) Except as otherwise provided in subsections (4) and (5), a custodian does not cease to be a custodian with respect to a record of personal health information until complete custody and control of the record, where applicable, passes to another person who is legally authorized to hold the record and the duties imposed by this Act and the regulations on a custodian with respect to personal health information shall continue to apply until the passage of custody and control of the record.</p> <p>NF advises that written notification to the regulator of physician practice is required when a physician is ceasing practice – physicians must indicate where the records will be stored, and or who has received transferred medical records.</p>
<p><b>Snooping – Unauthorized Viewing of PHI</b></p>	<p>*</p>
<p><b>Mismanaged PHI and Abandoned Records</b></p>	<p>The Act provides specific ability for records to be taken control of if a custodian does not comply with the duties imposed by the Act - section 4(4).</p> <p>4(4) Where a custodian fails to carry out his or her duties, the minister may appoint a person to act in place of the custodian until custody and control of the record fully passes to another person and may recover the costs and expenses of and incidental to the appointment from the custodian.</p> <p>The Act contains provisions requiring a custodian to notify individuals if records of their PHI are stolen, lost or improperly disclosed or accessed. (section 15)</p>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Existing Offences/Penalties and Enforcement Approaches</b></p>	<p>Offences for willful actions taken to access information improperly by any person. Also offences for breaches of the Act by custodians:</p> <p>88(1) A person who wilfully</p> <ul style="list-style-type: none"> <li>(a) obtains or attempts to obtain another individual’s personal health information by falsely representing that the person is entitled to the information;</li> <li>(b) makes a false statement to, or misleads or attempts to mislead, the commissioner or another person performing duties or exercising powers under this Act;</li> <li>(c) obstructs the commissioner or another person performing duties or exercising powers under this Act; or</li> <li>(d) destroys or erases personal health information with the intent to evade a request for access to the information,</li> </ul> <p>is guilty of an offence and liable, on summary conviction, to a fine of not more than \$10,000 or to imprisonment for a term not exceeding 6 months, or to both.</p> <p>(2) A custodian or information manager who</p> <ul style="list-style-type: none"> <li>(a) collects, uses or discloses personal health information contrary to this Act;</li> <li>(b) fails to protect personal health information in a secure manner as required by this Act; or</li> <li>(c) discloses personal health information contrary to this Act with the intent to obtain a monetary or other material benefit or to confer such a benefit on another person,</li> </ul> <p>is guilty of an offence and liable, on summary conviction, to a fine of not more than \$10,000 or to imprisonment for a term not exceeding 6 months, or to both.</p>
<p><b>Designated Archives (Decisions Related to PHI Issues)</b></p>	<p>*</p>
<p><b>Strict Liability and Identified Concerns</b></p>	<p>Due diligence offence available for custodian who improperly uses, collects, or fails to properly protect PHI in 88(3):</p> <p>88(3) A custodian or information manager shall not be found to have contravened paragraph (2)(a) or (b) if the custodian or information manager can establish that all reasonable steps were taken to prevent the contravention.</p>
<p><b>Educational Materials / Training</b></p>	<p>NL PHIA training materials for PHIA custodians have been published on the Department of Health’s website at: <a href="http://www.health.gov.nl.ca/health/PHIA">www.health.gov.nl.ca/health/PHIA</a></p>

## Nova Scotia

### Personal Health Information Act

<p><b>Purpose of Legislation</b></p>	<p>2 The purpose of this Act is to govern the CUD, retention and destruction of PHI in a manner that recognizes both the right of individuals to protect their PHI and the need of custodians to CUD PHI to provide, support and manage health care.</p>
<p><b>Trustee / Custodian Definitions</b></p>	<p>3 (f) “custodian” means an individual or organization described below 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:</p> <ul style="list-style-type: none"> <li>(i) a regulated health professional or a person who operates a group practice of regulated health professionals,</li> <li>(ii) the Minister,</li> <li>(iii) repealed</li> <li>(iv) a district health authority under the <i>Health Authorities Act</i>,</li> <li>(v) the Izaak Walton Killam Health Centre,</li> <li>(vi) the Review Board under the <i>Involuntary Psychiatric Treatment Act</i>,</li> <li>(vii) a pharmacy licensed under the <i>Pharmacy Act</i>,</li> <li>(viii) a continuing-care facility licensed by the Minister under the Homes for Special Care Act or a continuing-care facility approved by the Minister,</li> <li>(ix) Canadian Blood Services,</li> <li>(x) any other individual or organization or class of individual or class of organization as prescribed by regulation as a custodian.</li> </ul>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>How does Trustee Extend to Affiliates and Other Bodies?</b></p>	<p>Employees and third party contractors are agents of custodians under the legislation.</p> <p>3(a) “agent”, in relation to a custodian, means a person who, with the authorization of the custodian, acts for or on behalf of the custodian in respect of PHI for the purposes of the custodian, and not the agent’s purposes, whether or not the agent has the authority to bind the custodian, is paid by the custodian or is being remunerated by the custodian, and includes, but is not limited to, an employee of a custodian or a volunteer who deals with PHI, a custodian’s insurer or a lawyer retained by the custodian’s insurer;...</p> <p>The Act provides rules on the responsibilities of agents to custodians in section 28:</p> <p><b>28 (1)</b> A custodian is responsible for personal health information in the custody or control of the custodian and may permit the custodian’s agent to collect, use, disclose, retain, destroy or dispose of personal health information on the custodian’s behalf only if</p> <ul style="list-style-type: none"> <li>(a) the custodian is permitted or required to collect, use, disclose, retain, destroy or dispose of the information, as the case may be;</li> <li>(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 not contrary to the limits imposed by the custodian, this Act or another law; and</li> <li>(c) the prescribed requirements, if any, are met.</li> </ul> <p><b>(2)</b> Except as permitted or required by law and subject to the exceptions and additional requirements, if any, that are prescribed, an agent of a custodian shall 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).</p> <p><b>(3)</b> An agent of a custodian shall notify the custodian at the first reasonable opportunity if personal health information handled by the agent on behalf of the custodian is stolen, lost or accessed by unauthorized persons.</p>
<p><b>Trustee/Custodian Responsibilities and Compliance Methods</b></p>	<p>49 (2) At the expiry of the relevant retention period, PHI that is no longer required to fulfill the purposes identified in the retention schedule must be securely destroyed, erased or de-identified.</p> <p>NS advises that physician regulatory body should be notified of the location of the stored records and means by which patients can access them when physicians exit practice.</p>
<p><b>Snooping – Unauthorized Viewing of PHI</b></p>	<p>Offence for willfully attempting to or gaining access to Information in contravention of Act.</p>
<p><b>Mismanaged PHI and Abandoned Records</b></p>	<p>*</p>

\* Sections have intentionally been left blank where there was no applicable legislation, the information did not correspond with the criteria of the scan, or no information is available.

<p><b>Existing Offences/Penalties and Enforcement Approaches</b></p>	<p>106 A person is guilty of an offence if the person</p> <ul style="list-style-type: none"> <li>(a) wilfully collects, uses or discloses health information in contravention of this Act or the regulations;</li> <li>(b) wilfully gains or attempts to gain access to health information in contravention of this Act or the regulations;</li> <li>(c) wilfully obtains or attempts to obtain another individual's personal health information by falsely representing that the person is entitled to the information;</li> <li>(d) fails to protect personal health information in a secure manner as required by this Act;</li> <li>(e) in connection with the collection, use or disclosure of personal health information or access to a record of personal health information makes an assertion, knowing that it is untrue, to the effect that the person is a person who is entitled to consent on behalf of another individual;</li> <li>(f) wilfully disposes of a record of personal health information in contravention of the requirements for protection of personal health information required in this Act or the regulations;</li> <li>(g) requires production of or collects or uses another person's health card number in contravention of this Act or the regulations;</li> <li>(h) wilfully alters, falsifies, conceals, destroys or erases any record, or directs another person to do so, with the intent to evade a request for access to the record;</li> <li>(i) wilfully obstructs, makes a false statement to or misleads or attempts to mislead the Review Officer or another person in the performance of the duties, powers or functions of the Review Officer under this Act;</li> <li>(j) wilfully obstructs, makes a false statement to or misleads or attempts to mislead another individual or organization in the performance of the duties, powers or functions of that individual or organization under this Act;</li> <li>(k) uses individually identifying health information to market any service for a commercial purpose or to solicit money unless the individual who is the subject of the health information has expressly consented to its use for that purpose;</li> <li>(l) discloses personal health information contrary to this Act with the intent to obtain a monetary or other material benefit or to confer such a benefit on another person; or</li> <li>(m) breaches the terms and conditions of an agreement entered into with a custodian under this Act.</li> </ul>
<p><b>Designated Archives (Decisions Related to PHI Issues)</b></p>	<p>*</p>
<p><b>Strict Liability and Identified Concerns</b></p>	<p>*</p>
<p><b>Educational Materials / Training</b></p>	<p>*</p>

- APR** Abandoned Patient Records
- IMSP** Information Management Service Provider
- CUD** Collection, Use and Disclosure
- PHI** Personal Health Information

