



April 11, 2007

The Honourable P. Myron Kowalsky
Speaker of the Legislative Assembly
Rm 129 Legislative Building
2405 Legislative Drive
REGINA SK S4S 0B3

Dear Mr. Speaker:

Re: *The Health Information Protection Regulation Amendments*

I write today to offer commentary on the recent amendments to *The Health Information Protection Regulations* (Regulations). I am requesting that this be tabled in the Legislative Assembly pursuant to section 52 of *The Health Information Protection Act* (HIPA) which provides as follows:

52 The commissioner may:

(a) offer comment on the implications for personal health information of proposed legislative schemes or programs of trustees;

...

(c) in appropriate circumstances, comment on the collection of personal health information in a manner other than directly from the individual to whom it relates;

...

(e) comment on the implications for protection of personal health information of any aspect of the collection, storage, use or transfer of personal health information.

Further authority for tabling this letter can be found in section 33 of *The Freedom of Information and Protection of Privacy Act* (FOIP) which provides as follows:

33 The commissioner may:

(a) offer comment on the implications for privacy protection of proposed legislative schemes or government programs;

(d) from time to time, carry out investigations with respect to personal information in the possession or under the control of government institutions to ensure compliance with this Part.

The purpose in providing our commentary is to ensure the Assembly has a complete understanding of the impact or the potential impact of the new Regulations on Saskatchewan's health information trustees and residents.

Cancer Agency

The first amendment corrects a flaw in the previous Regulations section 2(c), which referred to the Saskatchewan Cancer Foundation and *The Cancer Foundation Act*. This is an important correction, and is consistent with recommendations from our office in our Investigation Report H-2005-002.¹ The definitions have been updated to reflect the name of “Saskatchewan Cancer Agency”, as well as the correct legislative instrument, “*The Cancer Agency Act*”.

Coroner

The amendment to the provision regarding the Coroner is clear. As amended, section 5.1 (2) reads:

(2) For the purposes of clause 27(4)(p) of the Act, the minister or a trustee may disclose personal health information, without the consent of the subject individual, to the chief coroner or a coroner appointed pursuant to The Coroners Act, 1999 with respect to the conduct of an investigation or inquest by the chief coroner or other coroner pursuant to that Act.

It is necessary to refer to section 3 of *The Coroners Act, 1999* which reads as follows:

Purpose

3 The purpose of this Act is to facilitate a coroner system that:

- (a) provides for independent and impartial investigations into, and public inquests respecting, the circumstances surrounding unexpected, unnatural or unexplained deaths;*
- (b) determines the identity of a deceased person and how, when, where and by what means that person died;*
- (c) uncovers dangerous practices or conditions that may lead to death;*

It is consistent with section 3 of *The Coroners Act, 1999*, that the Coroner would require the personal health information (phi) of a deceased individual. However the new regulation 5.1(2) does not limit disclosure or collection specifically to those who are deceased. Rather it uses very broad language to describe the provisions under which phi may be collected or disclosed “...with respect to the conduct of an investigation or inquest...”. We understand that the Coroner has very limited and specific situations that would require access to phi of a living person. As HIPA is paramount to *The Coroner’s Act, 1999* this amendment appears necessary to facilitate the function of the Coroner system.

¹ Page 15, available at <http://www.oipc.sk.ca/>

Disclosure to law enforcement

The amendments in section 5.1(1)(a) authorize disclosure by the Minister, without consent, of phi to:

to a member of the Royal Canadian Mounted Police, or to a member of a police service within the meaning of The Police Act, 1990, in the following circumstances:

(i) the personal health information is required to locate the subject individual for any of the following purposes:

(A) enforcing an outstanding warrant for arrest that has been issued by a court, person or body that has the lawful authority to issue that warrant;

(B) serving a subpoena with respect to the prosecution of an indictable offence;

(C) locating a person reported missing...

Prior to commenting specifically on this section of the Regulations, it is important to acknowledge two fundamental principles that our office applies; consistent with the principles applied by oversight offices across Canada:

- 1) The primary purpose to collect or use or disclose phi is the diagnosis, treatment and care of Saskatchewan residents. Use or disclosure of this information for purposes other than diagnosis, treatment or care is for a secondary purpose, and should normally occur only with consent of the individual.²
- 2) Exceptions to the 'consent rule' should be restricted to narrow and specific circumstances³. Proponents of the sharing of phi for non-health related purposes should bear the burden of establishing that:
 - The objective is sufficiently important to warrant overriding a constitutionally protected right of privacy; and
 - The proposed regulation is reasonable and reasonably justified. This would require that:

² CIHR Best Practises for Protecting Privacy in Health Research – September 2005, Elements 2,3 & 6

³ Alberta Health Information Act Guidelines and Practises Manual - HIA01 2001, Sec. 8.5, p. 200

- a) The proposed regulation is fair and not arbitrary, carefully designed to achieve the objective in question and rationally connected to that objective;
- b) The proposed regulation should impair the right of privacy as little as possible; and
- c) The proposed regulation should be proportional to the objective.

It is through this filter that we view the amended Regulations.

(A) Enforcing a warrant for arrest

Section 27(4)(i) of HIPA currently allows disclosure, without consent, “...where the disclosure is made for the purpose of commencing or conducting a proceeding before a court or tribunal...”. The purpose of a warrant is to secure the attendance in court in relation to some court proceeding. Since the provision already exists within HIPA, there is no need for this to appear within the Regulations, and will likely serve to confuse, rather than to clarify the Act.

(B) Serving a subpoena

Since we are dealing with indictable offences, Part XXII of the *Criminal Code* is relevant. Serving a subpoena “with respect to the prosecution of an indictable offence” relates to a court proceeding. It is hard to imagine that, at that stage, the police would not have more accurate information about the whereabouts of some witness. This appears to be a matter of convenience, not necessity. If there should be some unusual circumstance that warrants the need for disclosure of a witness’ phi by the Minister, presumably a court would be prepared to issue that order.

(C) Missing person

It is difficult to understand the rationale for this regulation in the context of HIPA. To begin, what constitutes a “missing person”? If a competent, sovereign individual of legal capacity chooses to leave his or her home, job, or community, I am not aware that they have any legal obligation to report this decision to anyone, including spouse, family or co-workers. In the absence of such an obligation on any of us, I cannot find the basis for permitting this disclosure by the Minister. This “missing person” may be a woman leaving an abusive relationship, or a prostitute fleeing her pimp, or any of countless other examples that perhaps warrant support and assistance but do not warrant disclosure of their phi (including registration information) without their consent. Without clear

grounds for this discretionary disclosure, this amendment will likely confuse, rather than clarify.

I note that none of the other three provinces with a stand-alone health information law authorize disclosure of phi without consent for purposes of locating a missing person.

Section 5.1(1)(b) and (c)

The amendments in section 5.1(1)(b) authorize disclosure by a trustee to police if it is requested for:

- (A) *enforcing the Criminal Code or the Controlled Drugs and Substances Act (Canada);*
- (B) *carrying out a lawful investigation pursuant to the Criminal Code or the Controlled Drugs and Substances Act (Canada);*

This is a broad ‘disclosure without consent’ provision, and the thresholds seem low. What is intended by the phrase “*enforce the Criminal Code*”? Does this require that a formal investigation already be initiated, or simply that any activity related to bringing perpetrators to justice would be sufficient to trigger disclosure?

The *Criminal Code* has more than 300 sections, and captures a long list of offences, many of which can be proceeded against by summary conviction and may be of a less serious nature. The majority of offences do not deal with physical injury to individuals. Offences that will be caught by this amendment include spreading false news, or loitering in a public park. It does not make sense to treat all offences and provisions contained in the *Criminal Code* in such an indiscriminate fashion. This broad amended regulation appears at odds with the Assembly’s preamble to HIPA.

We are concerned that section 5.1 of the Regulations does not conform with the protection of privacy offered through the *Charter of Rights and Freedoms* (Charter) as provided by the Supreme Court of Canada interpretation of sections 7 and 8 of the Charter. I refer you to the enclosed article, “Healing, not Squealing” recently published in the *Health Law Review*⁴. In it, the authors analyze portions of Alberta’s *Health Information Act* (HIA). Section 37.3 of this legislation is the counterpart to section 27(4) of HIPA and the recent amendments to the Regulations. The effective purpose of this Alberta provision is to allow secondary disclosure, without consent, of phi for law enforcement purpose. The Alberta section is as follows:

⁴ Health Law Review Volume 15, Number 2 (2007)

37.1(1) A custodian may disclose individually identifying health information referred to in subsection (2) without the consent of the individual who is the subject of the information to a police service or the Minister of Justice and Attorney General where the custodian reasonably believes

- (a) that the information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada, and*
- (b) that the disclosure will detect or prevent fraud or limit abuse in the use of health services*

(2) A custodian may disclose the following information under subsection (1):

- (a) the name of an individual;*
- (b) the date of birth of an individual;*
- (c) the nature of any injury or illness of an individual;*
- (d) the date on which a health service was sought or received by an individual;*
- (e) the location where an individual sought or received a health service; or*
- (f) whether any samples of bodily substances were taken from an individual.*

(3) If a custodian discloses individually identifying health information about an individual under subsection (1), the custodian may also disclose health services provider information about a health services provider from whom that individual sought or received health services if that information is related to the information that was disclosed under subsection (1).

(4) Health services provider information may be disclosed under subsection (3) without the consent of the health services provider who is the subject of the information.

In the aforementioned article, the authors analyze the many legal issues concerning disclosure, without consent, of phi for law enforcement purposes. We believe this article describes the significant concerns that the amendments to the Regulations create, and

clearly describes the legitimate issue of whether these amendments conform to the Charter. The authors comment that:

In exercising the discretion afforded by s. 37.3, health information custodians will inevitably disclose information that police could not have obtained without using (and conforming to the strictures of) their Criminal Code search and seizure powers. In La Forest's view, this kind of complicity is not permitted by the constitutional division of powers.

...

There is little question that at least some of the information subject to disclosure under s.37.3 would attract a reasonable expectation of privacy. From the earliest stages of its s. 8 jurisprudence, the Supreme Court of Canada has recognized the dangers of allowing health information to flow freely from practitioners to police.

...

The Supreme Court of Canada has set out a number of factors to be considered in making reasonable expectation of privacy decisions, but the most important in the context of informational privacy is whether the intrusion invades the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state." Some categories of information subject to disclosure under s. 37.3 ... would always satisfy this test and, thus, attract a reasonable expectation of privacy. The other categories (the individual's name and date of birth; the date on which a health service was sought or received by an individual; and the location where an individual sought or received a health service) will also often attract such an expectation.

...

But while warrantless searches are presumptively unreasonable, the Supreme Court has upheld them in a variety of situations. ...Section 37.3 falls into neither of these categories.

It concludes with the following:

We therefore recommend that s. 37.3 be repealed. If this does not occur, then the negative effects of the law could be mitigated in two ways. First, the constitutionality of the law could be challenged in the courts. Affected organizations, such as health regions and professional associations, could apply to a court for a declaration of constitutional validity. Alternatively, such a declaration could be sought by a criminal defendant prosecuted on the basis of information obtained under s 37.3.

Second, we recommend that professional associations and regional health authorities implement directives and procedures to strictly limit the disclosure of health information to police. To minimize the risk of improper disclosure, front-line health care providers should therefore be instructed to never release health information directly to police, unless: (i) the patient consents; (ii) the police present a valid warrant or other legal authorization compelling disclosure; or (iii) it is clear that the disclosure would avert or minimize an imminent risk to the health and safety of others.

Pan-Canadian Personal Health Information Privacy and Confidentiality Framework

*The Pan-Canadian Personal Health Information Privacy and Confidentiality Framework (Pan-Canadian Framework)⁵ has been adopted by all Canadian provinces other than Saskatchewan and Quebec. It has been described as “a common approach to protecting personal health information”. Its core provisions are consistent with the requirements of the Charter as well as the *Personal Information Protection and Electronic Documents Act* (PIPEDA), while taking into consideration the requirements and operational realities of the health system. The relevant exceptions to the consent requirement appear in the Appendix as follows:*

9.1 To another custodian where the custodian that is disclosing the information has a reasonable expectation that the disclosure will prevent fraud, limit abuse in the health services or prevent the commission of an offence under an enactment of a province/territory or Canada

9.4 To any person if the custodian believes on reasonable grounds that the disclosure will avert or minimize an imminent danger to the health or safety of any person.

The new Regulations allow more non-consented disclosure of phi for secondary purposes than is contemplated by the Pan-Canadian Framework.

Function Creep

Each time Saskatchewan Health champions a new kind of disclosure, use, or collection of phi for a purpose wholly collateral to the diagnosis, treatment and care of a patient, it also issues a message. The message is that there is every reason for a citizen to expect that their phi will be exposed to persons and agencies completely unrelated to the provision of diagnosis, treatment and care. It could be to identify truant children and track them, or it could be to facilitate law enforcement activities generally. Or it may be all kinds of other

⁵ Available at http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index_e.html

purposes that may be identified and then facilitated in the future. This can have the effect of undermining public confidence of citizens towards trustees, the health care system in general and even law enforcement. This becomes an even more serious matter when one considers how important it will be for Saskatchewan residents to be very confident that their privacy will be protected as this province proceeds with the development of the Electronic Health Record.

This set of regulations evidences a phenomenon known as ‘function creep’. In other words, an individual provides phi including registration information to a trustee presumably for the purpose of diagnosis, treatment and care. For a variety of reasons, not the least of which is the comprehensive nature of the Saskatchewan Health database, new applications and uses are identified for further sharing of this phi for entirely secondary purposes.

In recent testimony before the Standing Committee on Intergovernmental Affairs and Infrastructure, we note with interest the following statement by a Chief of Police: “...sometimes we have to threaten some [hospital] staff to arrest them for obstruction.”⁶ We fail to understand how, or why, a police officer would threaten a health official who likely believes they are acting in accordance with their ethical and legislated responsibilities.

We respect the role and the importance of our law enforcement agencies. We know that law enforcement provides an important service, and that their work is difficult. We recognize that the amendments to the Regulations are intended to make it easier for police. Yet their work is intended to be difficult by the very design of our legal system.

*It cannot be disputed that the [illegal activity] is odious, and poses a grave threat to society. And I therefore agree that all reasonable steps must be taken to eradicate it. But we cannot allow the desirability of these efforts to make the courts deviate from their high duty to ensure that those who wield power on behalf of the state must do so within the limits the Charter dictates for the benefit of the individual. No matter how grave the threat, law enforcement must operate in conformity with the enshrined protections of the Charter.*⁷

The Charter and the courts have created checks and balances to protect the rights of the individual. It is a long-standing principle within our society that we should not encroach upon these rights except under exigent circumstances where there is significant evidence

⁶ Saskatchewan, Legislative Assembly, Standing Committee on Intergovernmental Affairs and Infrastructure, “Hansard Verbatim Report”, No. 34 (February 5, 2007) at 547

⁷ R. v. Silveira, [1995] 2 SCR 297, La Forest J. (dissenting) 91.

of imminent harm. Our office remains unconvinced that sufficient justification has been provided for these regulatory amendments in section 5.1(1).

Bringing Saskatchewan Legislation in-line with other Provinces

The March 28th media release from Saskatchewan Health stated “*that Ontario, Manitoba, Alberta and British Columbia have operated with similar regulations for years, and that it will improve communication between the health sector and police agencies in Saskatchewan.*” We believe that both cross-Canada harmonization and improved communication are laudable objectives. Our office continually reinforces that goal by interpreting HIPA, FOIP, or LA FOIP consistent with our Canadian peers, wherever permitted by the legislation.

In the interests of harmonization, however, we note that in Ontario, Manitoba, Alberta and British Columbia, law enforcement agencies are included within the scope of their FOIP legislation. That means that citizens in those jurisdictions can go to the Information and Privacy Commissioner if they are denied access to their own information, if errors in that information are not corrected or if they think their personal information has not been properly collected, used or disclosed. In Saskatchewan, the only law enforcement bodies subject to FOIP or LA FOIP would be Saskatchewan Justice and the Saskatchewan Police Commission. Uniquely among Canadian provinces, Saskatchewan and PEI municipal law enforcement agencies are not subject to any access and privacy legislation and additionally not subject to independent OIPC oversight. Conversely, citizens in communities where police services are provided by the RCMP will have the benefit of the rights codified in the federal *Privacy Act*⁸ and *Access to Information Act*⁹. This produces an unequal level of access and privacy protection for Saskatchewan residents, not just when compared to other provinces, but even within our borders.

Information that is held by the police is, and should be, of interest to the communities they serve. Police agencies need to be accountable to citizens and that includes being accountable for the information in their possession or control. In all other Canadian provinces (other than PEI) that is achieved by making police services subject to the same access and privacy law as all other public sector organizations.

It appears that the position of the Saskatchewan Government is that the information rights of residents under *The Police Act, 1990* are somehow equivalent to the rights they would otherwise enjoy under FOIP and LA FOIP.

⁸ *Privacy Act* (R.S.C., 1985, P-21)

⁹ *Access to Information Act* (R.S.C, 1985, c. A-1)

There are two major areas where I think the Saskatchewan public loses by not having municipal police services treated like any other Saskatchewan public body that is subject to FOIP:

(1) FOIP Coordinator within the public body

Every public body should have a designated FOIP Coordinator who manages the access and privacy file within that body. For a police service this would include the following duties:

- Reports to the Chief and provides direct advice on access and privacy matters generally and FOIP compliance in particular;
- Develops policies and procedures to ensure FOIP compliance by the police service;
- Ensures appropriate training of all police staff so that they are familiar with legislative requirements, protocols, and best practices;
- Ensures that privacy complaints, access requests and correction requests are dealt with appropriately and expeditiously; and
- Liaises with our office to promote collaboration, consultation and cooperation between our oversight role and the police service to achieve full statutory compliance.

The municipal police service in every major city in Canada to our knowledge has someone designated as FOIP Coordinator or the equivalent. These individuals acquire expertise and specialized skills that benefit the entire police service.¹⁰

It is important to note that although the role of FOIP Coordinator is common in Canadian jurisdictions where police are captured by FOIP laws, there is nothing equivalent under *The Police Act, 1990*.

The need for access and privacy training among municipal police services in Saskatchewan was evident during testimony provided by a number of senior police

¹⁰ The Calgary Police Service, through its FOIP Coordinator, handles more than 400 access and privacy requests annually, of which more than 99% are successfully resolved at a local level. The Edmonton Police Service shares the same level of success, with a typical annual average of 210 requests.

officers testifying before the Standing Committee on Infrastructure and Government Relations with respect to Bill 20.

One Chief of Police observed at the Committee hearing on February 5, 2007 as follows:

*The police are governed under The Police Act in Saskatchewan to ensure confidentiality of information and thereby follow similar rules and regulations imposed on the medical profession. We are held accountable by law should such confidentiality be breached.*¹¹

The next day another police witness stated:

As I said before, we're governed by the Saskatchewan police [sic] Act which is, I mean that's I guess the bible to which we do our job. And within that we have some very strict guidelines around what we can and can't do and privacy issues are obviously one of them.

*...Well the fact that police fall under the Police Act [and not FOIP] is no different. Make no mistake about it, we have strict consequences if we breach confidentiality.*¹²

These police witnesses appear to be unfamiliar with the difference between privacy (right of an individual to exercise control over his or her personal information) and confidentiality (the protection of personal information once obtained against improper or unauthorized use or disclosure). The suggestion that police in any way operate under the same rules as the medical profession, namely the code of ethics, Canadian Medical Association Privacy Policy and the generous provision for non-consented sharing of personal health information for the purpose of diagnosis, treatment and care in HIPA, is simply inaccurate.

The same Chief of Police also told the Standing Committee that even if a stabbing or gunshot wound was reported to police under Bill 20 and it was determined that no criminal offence had occurred, the information “*would still be in our police data bank; there's no doubt about that. Any file that we do have, it's always there. It's always kept on file.*”¹³ Such a practice contravenes a number of privacy principles including the

¹¹ Saskatchewan, Legislative Assembly, Standing Committee on Intergovernmental Affairs and Infrastructure, “Hansard Verbatim Report”, No. 34 (February 5, 2007) at 545

¹² Saskatchewan, Legislative Assembly, Standing Committee on Intergovernmental Affairs and Infrastructure, “Hansard Verbatim Report”, No. 35 (February 6, 2007) at 571

¹³ Saskatchewan, Legislative Assembly, Standing Committee on Intergovernmental Affairs and Infrastructure, “Hansard Verbatim Report”, No. 34 (February 5, 2007) at 548

accuracy principle, the limiting rule for collection, use and disclosure and limits on secondary use or disclosure without consent. It is certainly inconsistent with the FOIP requirements that apply to all other public sector organizations in Saskatchewan.

Another police officer with one of the larger municipal police forces stated to the same Standing Committee as follows:

When police officers are hired, we take an oath of secrecy and confidentiality, and privacy is drilled into officers from day one. So our reporting systems are safe. They're secure, and we know what confidentiality is. Without sounding corny, privacy, confidentiality, security is our life. It's like saying danger is my middle name, but that's the reality. That is the case. We deal with issues every day that are safe and secure and not for public consumption.¹⁴

It is clear from reading Hansard that the police officer conflated privacy, confidentiality and security and had little appreciation for the right of any citizen to assert any measure of control over sharing information in the first place. Presumably, because municipal police services are not subject to FOIP, there would not have been formal privacy training for officers. It would not be surprising that many officers may not be clear on basic privacy concepts and best practices.

That same police officer misquoted HIPA's section 27(4)(a) as follows:

And I know reference was made to that section that is in HIPA right now, which I believe is section 27(4)(a), which the legislation there says that they may contact or disclose to the police if it's in the public interest. And perhaps this legislation wouldn't even be necessary if that was changed to shall – if the word may was changed to shall. I mean that's a minor change that would make a fairly big difference. But they are expected report suspected child abuse and domestic abuse and should report anything that is criminal in nature.¹⁵

The quotation above also evidences a questionable grasp of the statutory and common-law responsibilities of any health care provider in Saskatchewan.

Again, the same officer observed that:

¹⁴ Saskatchewan, Legislative Assembly, Standing Committee on Intergovernmental Affairs and Infrastructure, "Hansard Verbatim Report", No. 35 (February 6, 2007) at 567

¹⁵ Saskatchewan, Legislative Assembly, Standing Committee on Intergovernmental Affairs and Infrastructure, "Hansard Verbatim Report", No. 35 (February 6, 2007) at 567

*We gather intelligence all the time. That intelligence is constantly shared within our police department, within the different sections and plays a huge role in how we do our job. So finding out who did it and charging the person obviously is optimal, but just because that doesn't happen doesn't mean that it wasn't important that we be called.*¹⁶

It seems reasonably clear from the testimony from police witnesses to the Standing Committee that police witnesses spoke to an appropriate concern with not sharing personal information outside of the police service, but no concern whatsoever with a relatively unregulated flow of information sharing within the police service. There was no evidence provided by any of the police witnesses about how a 'need to know' policy works in a police service or the rule that the least amount of personal information necessary for the purpose originally identified be collected, used and disclosed. That testimony largely ignored the bigger issue of privacy.

(2) Specialized skills in OIPC as Oversight Body

As the oversight body for purposes of FOIP and LA FOIP, our office (the OIPC) has specialized skills and knowledge in the fast developing access and privacy fields. Our office manages a heavy caseload of exclusively access and privacy files and consequently develops strong expertise in access and privacy law and procedure. For example, an investigator (Portfolio Officer) in the OIPC must complete the University of Alberta Information Management Access and Privacy Certificate Program in order to work in this office. In addition, any new hire as a Portfolio Officer undergoes months of specialized training before they are tasked with providing advice and commentary or undertaking investigations and reviews on their own.

The high volume of cases and requests for assistance ensure strong familiarity with access and privacy law and practice. In the last fiscal year, our office addressed 2168 calls and email requests for advice and assistance from public bodies and the Saskatchewan public. We opened 93 different files dealing with a diverse range of access reviews and privacy investigations. In addition we provided more extensive advice and commentary on more than 95 files for different public bodies.

In the past 4 years, we have undertaken more than 400 reviews and investigations. Of the investigations completed, more than 80% have been successfully resolved

¹⁶ Saskatchewan, Legislative Assembly, Standing Committee on Intergovernmental Affairs and Infrastructure, "Hansard Verbatim Report", No. 35 (February 6, 2007) at 571

informally. Of the 15% that have resulted in a formal Report, approximately 90% of the recommendations made have been adopted either in whole or in part.

Additional Factors to Consider

The following are additional factors when considering the differences that making police services subject to FOIP would create:

- It is not clear to us that the municipal board of police commissioners or regional police boards, or the Public Complaints Commission will have the expertise, the experience and the tools to deal specifically with breach of privacy complaints that will be in any way equivalent to the way those complaints are dealt with when they relate to any other Saskatchewan public bodies subject to either the FOIP Act, the LA FOIP Act or HIPA. In the past, the Commission's investigator has referred to our office individuals who alleged that their privacy had been violated by members of a police service. I assume this was done with an expectation that our office would be more appropriate to deal with such complaints.

Obviously the staff of the Public Complaints Commission has strong investigative skills and the experience to deal satisfactorily with many types of complaints against members of any police service. It is important to realize that with the increasing complexity and sophistication of privacy challenges, issues and technologies, it is difficult to become expert at access and privacy issues when that is not your area of specialization.

- I cannot find in *The Police Act, 1990* any explicit reference to breach of privacy, the tests or the standards that would be used in assessing an alleged breach of privacy.
- I can find no reference to any requirement that the complainant's identity will consistently be protected as the personal information of the complainant and only shared on a limited basis with those persons who have a demonstrable need to know. It appears that decisions about the way in which a complainant's personal information, or that of any other civilian who may be involved, will be determined at the discretion of hearing officers, or the Public Complaints Commission.
- The hearing officer is designated by the Minister of Justice and therefore would not be seen as independent of the Department as would an independent Officer of the Legislative Assembly. The Public Complaints Commission is appointed by the Government, not by the Legislative Assembly.

- The hearing process incorporates by reference the rules of evidence applicable in the Court of Queen's Bench. There is certainly not the kind of flexibility that exists for investigations of an alleged breach of privacy under FOIP. I accept that the more elaborate and formal procedure in *The Police Act, 1990* may be very appropriate for dealing with an array of complaints against police services and police officers. I do have questions as to whether this is the most appropriate and efficient way to deal with breach of privacy complaints made against police.

Conclusion

At the end of the day, any new regulation as 'subordinate legislation' needs to be assessed in terms of whether it is consistent with the enabling legislation, in this case HIPA.

The new regulation dealing with the Saskatchewan Cancer Agency and the Coroner's access to personal health information appear to be appropriate.

The new regulation 5.1(1), in my respectful opinion, is likely to negatively impact the privacy of the residents of Saskatchewan. I encourage the Assembly to revisit regulation 5.1(1) and revise it to restore the appropriate balance between privacy and the legitimate needs of law enforcement.

In the event that the Assembly resolves not to revise the new Regulation 5.1(1), then I respectfully urge the Assembly to ensure that, like all other Canadian provinces other than PEI, Saskatchewan municipal police services are brought within the scope of FOIP or LA FOIP. In that event, the concerns I have identified in this report would be mitigated to a large extent.

Honourable P. Myron Kowalsky
Page 17
April 11, 2007

My office is available to discuss these concerns with any Committee of the Assembly at your convenience.

Respectfully submitted,

A handwritten signature in black ink, appearing to be "R. Gary Dickson", written on a light gray rectangular background.

R. Gary Dickson, Q.C.
Saskatchewan Information and Privacy Commissioner

Enclosures (2)