



May 9, 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 Vital Statistics Act, 2007 (Bill 61)*

I write today to offer commentary on Bill 61, *The Vital Statistics Act, 2007* (Bill 61). I request 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 provide the Assembly with our assessment of the impact this Bill may have on access and privacy rights of Saskatchewan residents.

.../2

Our Collaboration with Saskatchewan Health

Saskatchewan Health (Sask Health) has utilized a proactive approach by consulting with our office early in the drafting process, and we applaud their efforts at proactive consultation. Bill 61 incorporates many recommendations provided by our office over a number of months. We believe it is a stronger piece of legislation in the result.

Statutory Mandate for Electronic Database

I note that in the April 11, 2007 Government of Saskatchewan media release entitled “*Improvements to the Vital Statistics Act*”¹ the intent was described as follows:

The intent is to update and clarify [The Vital Statistics Act, 1995] in a number of areas, including:

- *reflect the administrative and business processes employed by Vital Statistics, hospitals and funeral directors in the registering of vital events;*
- *add transparency concerning the rights of access to records and rules for the collection, use and disclosure of personal information collected by Vital Statistics;*
- *allow for the inclusion of co-parents on the statements of live birth and stillbirth;*
- *provide authority for funeral directors and hospitals to electronically notify vital statistics of births, stillbirths and deaths;*
- *provide authority for the maintenance of electronic registries and indexes of vital event registrations; and*
- *allow the permanent retention of vital event registration documents in an electronic database*

[Emphasis added]

¹ Available at <http://www.gov.sk.ca/news?newsId=ef0d39f4-11e6-4d42-8427-13851249c352>
.../3

Contemporary Saskatchewan Context

(1) Identity Theft

Identity theft is one of the most serious crimes in Canada and one that is increasing in both frequency and sophistication. Saskatchewan Justice Minister Frank Quennell spoke of the seriousness of identity theft in his March 12, 2004 news release, “*Saskatchewan Supports Identity Theft Initiatives*”.² The Minister’s news release described identity theft as follows:

Identity theft, one of the fastest growing crimes in the marketplace, occurs when someone uses a victim’s personal information, without their knowledge or consent, to commit a crime, such as fraud or theft. Identity thieves will steal wallets, redirect mail, rummage through garbage, set up telemarketing schemes, and break into computers in order to take money out of a bank account, go on shopping sprees, apply for loans, credit cards and social benefits, rent apartments and even commit more serious crimes—all in the victim’s name.

In addition to names, addresses and phone numbers, identity thieves look for social insurance numbers, driver’s licence numbers, credit card and banking information, bank cards, calling cards, birth certificates and passports.

Once they steal the information they need, identity thieves can manipulate it and invade their victim’s personal and financial lives. Victims of identity theft may incur damaged credit records, unauthorized charges on credit cards and unauthorized withdrawals from bank accounts. In many cases, victims must change their addresses, telephone numbers and even their social insurance numbers.

According to a 2006 poll conducted for CBC by the Strategic Counsel³, one in 6 Canadians is affected by identity theft either directly or within their household. The Canadian Council of Better Business Bureaus estimates that the cost to the Canadian economy associated with identity theft is \$2.5 billion per year.⁴

From the perspective of identity theft, one of the most important kinds of personal information is that which is contained in ‘cradle to grave’ type registries such as Vital Statistics. Birth and death certificates are frequently used as foundation documents to

² Available at <http://www.gov.sk.ca/news?newsId=8e921c19-1f9c-412e-9f40-ee1c49aabe18>

³ Available at <http://www.cbc.ca/consumer/story/2007/03/01/identify-fraud.html>

⁴ RCMP Powerpoint slide presentation entitled “Identity Theft- Commercial Crime Section”, Cst. Travis Adams (undated)

establish identity. According to RCMP, two of the three “key pieces of information” sought by the suspects to build a profile are Name and Date of Birth.⁵

In 2007, it is hard to imagine anything more important for a provincial Vital Statistics office than to take all reasonable measures to protect birth and death information and official certificates, to reduce the risk of identity theft. Confidence in the authenticity of such certificates is of fundamental importance, as is the protection of the personal information in the database.

(2) Data Matching

One of the systems that create opportunities for identity theft is data cross-referencing (data matching). Data matching is a term that captures cross-agency comparisons of personal information to improve data quality⁶. This includes linking person-specific data sets to produce new kinds of information in either an identified, de-identified or anonymized form.

As observed by Paul Chadwick, former Privacy Commissioner for Victoria, Australia:

*Addressing data matching is part of the larger challenge of ensuring that the collection and handling of personal information in a technological age is done according to long standing values, including respect for privacy. In its Information Privacy Principles, Victoria has adopted well known international data protection standards. This is partly to build trust, partly to keep a check on potential abuse of power, and partly to ensure that the necessary data continues to be available. If people lack trust in authorities, they do not believe that abuses can be detected and checked, then they begin to act in self-defence. They may provide false or incomplete data. This in turn reduces the quality of decisions based on the data. This is not in the public interest and, over time it will corrode the legitimate tasks of public administration, for which personal information aided by technology, is necessary.*⁷

Unlike more modern privacy laws, Part IV of FOIP includes no particular requirements before a government institution can data match. There are certainly no specific statutory safeguards to limit data matching in FOIP, such as exists in other jurisdictions.⁸ Indeed the permissive disclosures, without consent, in the FOIP Regulation include:

⁵ RCMP Powerpoint slide presentation entitled “Identity Theft- Commercial Crime Section”, Cst. Travis Adams (undated)

⁶ Victorian Public Sector Data Matching Audit February 2005. Available online at <http://www.privacy.vic.gov.au/dir100/pri>

⁷ *ibid*, page 6

⁸ Examples of data matching provisions can be found in Ontario’s *Personal Health Information Protection Act*, section 47 requires prior notice to the Information and Privacy Commissioner; Alberta’s *Health Information Act* sections 68 to 72 require approval by the Information and Privacy Commissioner before data matching can be undertaken; British Columbia’s *Freedom of Information and Protection of Privacy Act*, section 35(b)

16 For the purposes of clause 29(2)(u) of [FOIP], personal information may be disclosed:

- (a) to another government institution or a local authority for the purposes of:
 - (i) determining the eligibility of an individual to participate in a program of, or receive a product or service from, the Government of Saskatchewan, a government institution or a local authority, in the course of processing an application made by or on behalf of the individual to whom the information relates;*
 - (ii) verifying the eligibility of an individual who is or was participating in a program of, or receiving a product or service from, the Government of Saskatchewan, a government institution or a local authority;*
 - (iii) verifying the accuracy of personal information held by the other government institution or the local authority; or*
 - (iv) collecting a debt or assisting in the collection of a debt owing to Her Majesty in right of Saskatchewan, a government institution or a local authority;**
 - (b) to an individual or body providing consulting or other services to the Government of Saskatchewan or a government institution if the individual or body agrees not to make a subsequent disclosure of the information in a form that could reasonably be expected to identify the individual to whom it relates;*
- ...

Notwithstanding these provisions in FOIP, our general jurisdiction allows us to oversee both uses and disclosures of personal information by public bodies. We have, in all cases where FOIP applies, the opportunity to investigate and report.

(3) Development of the Electronic Health Record for Saskatchewan Residents

Canada Health Infoway (Infoway) has developed a national blueprint for an electronic health record (EHR) solution to be used by its provincial and territorial partners including Sask Health. In a recently published *White Paper on Information Governance of the Interoperable Electronic Health Record*⁹, one of the topics identified by Infoway that is related to the privacy rights of patients is as follows:

requires that “record linkage” must not be harmful to the individuals and the benefit to be derived from the record linkage must be clearly in the public interest. A similar provision can be found in section 72(1) of Alberta’s *Freedom of Information and Protection of Privacy Act*.

⁹ Page v; Available online at <http://www.infoway-inforoute.ca/en/ValueToCanadians/PrivacySecurity.aspx>

9. Secondary use – Over time, some EHR information may ultimately be used for secondary purposes such as public health surveillance and health system analysis and management. Some health information statutes permit such uses. However, should patients be informed of secondary uses? What level of de-identification, is needed before personal health information that was collected for the purpose of treatment and care can be fairly and ethically used for research without requiring patient consent? Is it feasible or reasonable to expect the EHR to include information that would specifically indicate whether a patient agrees to be contacted for the purposes of health research?

I have noted in other reports to the Assembly¹⁰ that as this province proceeds with the development of EHR, a great deal of attention needs to be focused on building patient confidence and trust in what happens and can happen with the personal health information (phi) of any individual. I have in past reports to the Assembly urged caution in expanding the list of non-consented uses and disclosures of phi for purposes that are unrelated to the diagnosis, treatment and care of the subject individual.

As noted earlier, data matching involves the matching of data about citizens held in different databases, such as EHR. Typically, decisions in Saskatchewan around matching are administrative decisions made by departmental personnel.

Areas of Positive Change

I wish to acknowledge again the consultations with our office initiated by Sask Health. We appreciated the opportunity to raise concerns in respect to certain elements of Bill 61 at an early date. We also appreciate the significant efforts by Sask Health to address many of our concerns before the introduction of Bill 61 in the Assembly. The positive changes include:

- Elimination of Division Registrars
- Clarity of Terminology
- Extension of time for appeals
- Restrictions on Disclosure
- Registration of abandoned newborn child
- Amendments to names

Eliminating the Role of Division Registrars

¹⁰ Letter to The Speaker: Bill 20 *The Gunshot and Stab Wounds Mandatory Reporting Act*, Nov. 6, 2006; Letter to The Speaker: *Health Information Protection Regulation Amendments*, Apr. 11, 2007; *Office of the Information and Privacy Commissioner 2005-2006 Annual Report*, Nov. 9, 2006 (all documents available at www.oipc.sk.ca)

The new legislation creates a centralized source of data through the elimination of division registrars and bringing their previously held information under the management of the Director. Section 6 of Bill 61 reads as follows:

Records of registrations

6(1) The director shall arrange in a systematic manner and, subject to section 8, shall permanently preserve:

- (a) all statements accepted for registration;*
- (b) all records submitted in support of any statement accepted for registration;*
- (c) all notations effecting an amendment or correction to a statement accepted for registration; and*
- (d) all records submitted in support of an amendment or correction to a statement accepted for registration.*

(2) The director shall prepare and maintain, in any format that the director considers appropriate, comprehensive and continuous indexes of live births, deaths, stillbirths and marriages registered pursuant to this Act or any former Act.

From a risk-management perspective, this makes good sense. It should significantly reduce security risks by merging multiple points of access into a single point. In the process, the legislation includes a section to specifically address the transfer of information during this transition. Section 109 reads accordingly:

Transitional—division registrars

109(1) In this section, “division registrar” means a person who, immediately before the coming into force of this Act, was a division registrar, as defined in subsection 2(1) of The Vital Statistics Act, 1995, or a deputy division registrar.

(2) On the coming into force of this Act, every division registrar shall immediately send to the director:

- (a) all registrations, records and documents that a division registrar is required to keep in a place of safety pursuant to clause 29(b) of The Vital Statistics Regulations;*
- (b) all copies of reports that a division registrar is required to keep as an office record pursuant to clause 29(g) of The Vital Statistics Regulations;*
- (c) all records pertaining to any application for the registration of an event pursuant to The Vital Statistics Act, 1995 that, on the coming into force of this Act, has not been completed; and*
- (d) all other records pertaining to the administration of The Vital Statistics Act, 1995 or any former Act and all copies of any records pertaining to the administration of The Vital Statistics Act, 1995 or any former Act.*

(3) Every person who knowingly contravenes subsection (2) is guilty of an offence and is liable on summary conviction to a fine of not more than \$10,000.

Sask Health has provided assurance that the transmittal of all data will be secure, although they have not provided details of how this will be accomplished. Given this lack of detail, section 109(3) becomes important since it should provide additional motivation to ensure it is achieved.

Clarity of Terminology

Early drafts included undefined terminology that appeared to be unique to Bill 61. We are pleased that Sask Health has also recognized this. We now see much clearer use of terminology, such as “*co-parents*”. We also see these terms defined within section 2 of Bill 61. This gives our office greater confidence that the application of Bill 61 will be consistently applied. I commend Sask Health for work that has been done to clarify definitions for certain phrases and terms that appeared in earlier iterations.

Extension of Time

Sections 83(2) and 84 describe procedures available to an applicant who has been refused, by the Director, amendments, searches or issuance of a certificate or extract. We are pleased to see that the time period to appeal this decision has been extended from 60 days to 1 year.

Restrictions on Disclosure

I congratulate Sask Health for changes that have been made to section 72 to impose restrictions on disclosure of information. This section explicitly reinforces the very limited ‘need to know’ principle that should exist in any legislation involving the disclosure of information. This principle requires that Vital Statistics should only disclose personal information to those that have a legitimate need to know. Furthermore, disclosure should be made of de-identified information, and resort to personal information only when de-identified information would not serve the primary purpose. We welcome this important change.

Areas of Continued Concern

Electronic Database

Bill 61 formally acknowledges the use of an electronic database to maintain records. Although this had been part of the department’s operations since 1979, it is now expressly authorized. This recognizes the critical role that the electronic database plays in the management and operations of Vital Statistics.

It is equally important to recognize that this database also creates an attractive warehouse of information for those who may not have authority to access the data, or may choose to use it

for unauthorized purposes. In addition, there may be demands for more use and disclosure but for secondary purposes that speak more to convenience than legitimate need. Our concerns with this database are consistent with concerns we have previously raised with other electronic databases.

In discussions with Sask Health, we asked the following questions:

- 1) Will the system have appropriate administrative, technical and physical safeguards?
- 2) Will the new database provide varying degrees of security and access to ensure that the least amount of personal information and personal health information necessary would be available to any given person?
- 3) Will there be appropriate monitoring and audits of database activity, as well as annual reporting of the frequency of different access, collections, use and disclosures?

We are especially concerned with a lack of detail in respect of monitoring and auditing of database activity. On this question, Sask Health advised they would heighten security provisions, and would consider developing audits and disclosure logs. To “*consider*” developing audits and disclosure logs is insufficient in current day experience. Audits, disclosure logs, and regular monitoring should be a primary requirement addressed during the design phase of any electronic database. It is not something to be considered after the fact. The absence of disclosure logs would make it nearly impossible to determine if unauthorized disclosure has occurred in the database. Further, if these logs are developed, then regular inspection and auditing must also occur. Each relies upon the other, and both are necessary.

Need for Explicit Security Provisions

As noted earlier, the indication that Vital Statistics is contemplating heightened security provisions and accountability measures provides little comfort. In my respectful submission this is the time to build in, as statutory requirements, audits and disclosure logs and other key security features in the new electronic database systems. Alternatively, if such items are not specifically incorporated into the legislation, there would at least be added value in having Vital Statistics outline the operational details of how this personal information and personal health information will be adequately protected in terms of collection, use and disclosure.

We have asked questions about the levels of different access/security that will be available or will apply to the electronic database. It is unclear what kinds of authentication and identity management tools are contemplated. We have been advised that appropriate safeguards have been or will be put in place through policy and procedures. Our office has

not seen those instruments nor have we seen a comprehensive, detailed Privacy Impact Assessment (PIA) that might otherwise have provided us with some measure of reassurance.

We refer to the recent and highly publicized case of intrusion into the databases of TJX. The attacker first broke into the databases in July of 2005, yet was not discovered until December of 2006. The damage, that TJX customers have and will continue to suffer, could have been mitigated substantially with appropriate auditing and monitoring of database disclosures.

Data Sharing Agreements

I understand from Sask Health that the intention is to address a number of the questions we have raised with respect to the Vital Statistics database by means of data sharing agreements. My recommendation is that given the importance of this database, Bill 61 should at least define the elements to be incorporated into such data sharing agreements. Also, as noted elsewhere in this report, a requirement for a comprehensive PIA would be helpful including a requirement that the PIA be shared with our office prior to adoption of the system of safeguards.

Paramountcy

In Bill 61, section 112 has the effect of making Part VIII of Bill 61 (Information Management) paramount to FOIP. This means that in the event that at some future date there is a conflict identified between Part VIII and any provision in FOIP such that to comply with one will result in a violation of the other then Part VIII will prevail.¹¹

There is a significant improvement in Bill 61 over previous iterations in that the paramountcy provision in Bill 61 has been scaled back so that FOIP is paramount for all purposes and provisions in Bill 61 except for Part VIII.

Nonetheless, it is Part VIII that most directly impacts the privacy and access rights of Saskatchewan residents.

Part VIII of Bill 61 addresses the following important activities:

- Who will get access to information in the database
- How registration information about Saskatchewan residents will be verified
- Safeguards
- Confidentiality
- Restrictions on disclosure
- Collection from Sask Health

¹¹ Paramountcy is discussed in more detail at page 7 of the *OIPC Submission to the WCB Committee of Review* dated October 24, 2006. This is accessible at www.oipc.sk.ca under the *What's New* tab.

- Use by Sask Health
- Collection of health services numbers
- Vital statistics information from other jurisdictions
- Information exchange agreements
- Disclosure and use agreements
- Information management services agreements
- Publication of statistical information

Given that FOIP is a comprehensive code governing the collection, use and disclosure of personal information for all other public bodies in Saskatchewan, the obvious question is what compelling reason exists to make all of the above listed activities paramount to FOIP.

As noted in the Canada Health Infoway EHR governance paper:

Finally, the public relies on federal, provincial and territorial governments to protect public interests by enacting privacy protective laws and regulations and by ensuring independent oversight, such as that provided by provincial and territorial Information and Privacy Commissioners. To be effective, accountability for personal health information needs to be clearly assigned throughout the EHR Infostructure.

[Emphasis added]

Since the impact of the paramountcy provision in section 112 will drastically shrink the scope of independent oversight as provided by this Office, it will be very important for the Assembly to be satisfied that such a denial of oversight can be justified by some more compelling public interest.

Linkage of Data With Health Services Number

I have a general concern about the universal linking of the health services number and the identity of parents to so many records. It is important to recognize that HIPA implicitly recognizes the special prejudice that attaches to any Saskatchewan resident's health services number. This relates to the role of that health services number as the "key" to access a significant body of personal health information about that resident in the custody or under the control of Sask Health. This recognition is manifest in section 11 of HIPA and the limitations imposed by that provision on the use and disclosure of the health services number. Section 11 provides as follows:

11(1) An individual has the right to refuse to produce his or her health services number or any other prescribed identifying number to any person, other than a trustee who is providing a health service, as a condition of receiving a service.

- (2) Except as provided in subsection (3), no person shall require an individual to produce a health services number as a condition of receiving any product or service.*
- (3) A person may require the production of another person's health services number:*
- (a) for purposes related to:*
 - (i) the provision of publicly funded health services to the other person;*
 - (ii) the provision of a health service or program by a trustee; or*
 - (b) where authorized to do so by an Act or regulation.*

I understand the primary purpose for this linkage is to ensure the accuracy of information. FOIP provides that any government institution is limited as to the personal information it collects and the manner in which it collects that information. The routine collection of information of parents' given name and place of birth as contemplated by Bill 61 certainly appears unwarranted. A comprehensive PIA would have been beneficial in ensuring a rigorous examination of the need to know. Such a PIA would presumably identify what alternatives exist to ensure accuracy without the need for general linkage through the health services number.

Health Research or Other Research Involving Personal Information

I note that the secondary purpose for the Vital Statistics database is to use the information for research. Ideally, that should require the consent of individuals. At the very least, it should require clear notification to citizens of the proposed secondary use and an opportunity to opt-out.

It is important to note that Vital Statistics may be a separate administrative unit within Sask Health but it has no separate standing under FOIP. In other words, FOIP does not recognize units within a department. Any personal information under FOIP or personal health information under HIPA that is in the possession of Vital Statistics or under its control is, for purposes of FOIP, in the possession or under the control of Sask Health. That same information when made available to other units within Sask Health is a "use" transaction and not a "disclosure" transaction. In the event that Sask Health wishes to utilize personal health information for "research", compliance with section 29 of HIPA is essential.

I am concerned that although Sask Health is a trustee for purposes of HIPA, not all of the personal information in the Vital Statistics database will qualify as personal health information within the meaning of section 2(m) of HIPA. In the result there would be no requirement for review by and approval from a Research Ethics Committee under HIPA with any research requiring only personal information.

There is however no comparable requirement for research with personal information of individuals under FOIP. I encourage the Assembly to address this gap in privacy protection. Obviously, this concern does not apply to de-identified or statistical information.

Largely Unfettered Discretion for Director

I broached with Sask Health a concern in earlier iterations of Bill 61 that there was a vast amount of discretion given to the Director but no specified criteria for the exercise of that discretion. I acknowledge that Bill 61 reflects some narrowing of the discretion of the Director. Nonetheless provisions such as section 26(3) still give very broad discretion to the Director. My suggestion is that specific criteria addressing the exercise of that discretion be incorporated into Bill 61.

I have raised concerns about section 28(2)(d) of Bill 61. I have been advised by the Department that this will not include DNA identification material and that information collected will not be entered into an electronic database. I encourage the Assembly to explicitly include these qualifications in Bill 61.

Unconsented Disclosure to Unrelated Persons

Section 60(2)(c) of Bill 61 is curious. It is unclear why police are entitled to information about an individual without consent to “*locate a person reported missing*”.¹² This begs the question of what happens to a legally competent adult who wishes to leave their community, and chooses to not disclose this plan and action to others. If the intention is to allow disclosure to police of the death registration of a missing person, then the section should be narrowed to that circumstance.

Disclosure to Foreign Governments

Section 61(4) of Bill 61 enables disclosure to foreign governments. This presumably should only be to advantage the individual. There should be safeguards to regulate this disclosure. We have not seen any particulars with respect to such safeguards.

Disclosure to Nearest Living Relative

Section 62(2)(i) of Bill 61 is presumably intended to accommodate a person such as a relative or perhaps someone with a close personal relationship to the deceased. I recommend that access to the cause of death should be available to those persons without the necessity of making an application to the court. This would parallel Section 27(4)(e) of HIPA.

¹² This example has been previously discussed in our Letter to The Speaker: *Health Information Protection Regulation Amendments* Apr. 11, 2007;

Disclosure to Police

Section 65(2) of Bill 61 permits the Director to waive those requirements for police or a prescribed law enforcement agency. It is apparently left to the discretion of the Director to assess both the identity of the requestor as well as that requestor's eligibility. This would be supported to some extent by section 65(4) of Bill 61. Municipal police services in Saskatchewan are not subject to FOIP or *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).¹³ That is a significant area of vulnerability in terms of privacy protection. To compensate for that gap in protection, the legislation should ensure considerably more rigour applies in determining disclosure to police.

Tracking Disclosures

I recommend that there should be a tracking capability and process to allow monitoring of Vital Statistics disclosures which occur without the consent of the individual.

Extensive Delegated Powers for Regulation

Given the breadth of the regulation-making power in section 100 of Bill 61, I encourage Sask Health to publish regulations in draft form before they go into force. This would permit our office and other interested parties an opportunity to comment

I trust that this commentary will be useful in the Assembly's deliberations with respect to Bill 61.

Yours truly,



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

¹³ See note 9 Supra