Office of the
Saskatchewan Information
and Privacy Commissioner

Best practices for Mayors, Reeves, Councilors, and School Board members in handling records that contain personal information and personal health information

Mayors, Reeves, Councilors, and School Board members (Elected Officials) who have a concern(s) and bring sensitive personal information (pi) or personal health information (phi) forward may not realize that this information is not protected under *The Freedom of Information and Protection of Privacy Act* (FOIP*), Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) nor *The Health Information Protection Act* (HIPA). The Saskatchewan Information and Privacy Commissioner has developed this document to assist Elected Officials in protecting the sensitive pi/phi that he or she collects.

Before proceeding, it is important to understand in what limited circumstances LA FOIP may apply to certain records. LA FOIP applies to records in the possession or control of a local authority. Municipalities and school boards are examples of local authorities. However, LA FOIP would not apply to records of Elected Officials if those are collected or generated in the course of conducting constituency business or political activities. If instead the Elected Official is engaged in carrying out the mandate or functions of the local authority, then LA FOIP most likely will apply to those records.

The second consideration is to determine if the records contain pi or phi.

What is personal information?

For a full definition of what is considered pi, see subsection 23(1) of LA FOIP. Generally, the following is considered pi:

- Information about an identifiable individual;
- Is personal in nature;
- The personal views or opinions offered by an individual are the personal information of that person;
- The personal views or opinions of one individual about another person is the personal information of the other person; and
- Employment history is considered personal information.

What is personal health information?

The definition of phi is found in HIPA under subsection 2(m):

> 2(m) "personal health information" means, with respect to an individual, whether living or deceased:

(i) information with respect to the physical or mental health of the individual;

(ii) information with respect to any health service provided to the individual;

(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;

(iv) information that is collected:

(A) in the course of providing health services to the individual; or

(B) incidentally to the provision of health services to the individual; or

(v) registration information;

What is a "record"?

Section 2(i) of FOIP describes a record as:

> . . . a record of information in any form and includes information that is written, photographed, recorded or stored in any manner, but does not include computer programs or other mechanisms that produce records;

Purpose and collection

Citizens and organizations consult Elected Officials on problems and issues they have with local government and/or the health system. In that process of asking for help, they may provide documents or give verbal information to Elected Officials which contains considerable sensitive pi/phi.

Before collecting any pi or phi, the Elected Official should pause and assess the purpose for collecting this information and whether this information is necessary for such a purpose.

In particular, consider documents that you may not need to collect such as tax returns, doctor's reports, financial statements, laboratory tests and non-relevant correspondence.

When an Elected Official talks to a citizen, have the citizen consent to your collecting, using or disclosing information and keep that consent on your file (either hardcopy or electronic). A written consent is the best, email consent is next best and consent over the telephone is least best. Telephone consent should be recorded in your notes.

Elected Officials should refrain from collecting more pi/phi than is necessary to fulfill the identified purpose. Once the purpose for which the information was being collected has been fulfilled, the pi/phi should be disposed of, unless otherwise required to be retained by law.

Elected Officials need to make informed choices about how long to keep pi/phi and when and how to dispose of it. The capacity and desirability to retain massive amounts of pi/phi indefinitely increases the risks and consequences of a potential data breach.

Retention Periods

With respect to records retention and disposal schedules, Elected Officials may want to consult with the Saskatchewan Archives Board. Contact information for the Board is available on its website, www.saskarchives.com.

A record retention and disposal schedule prescribes requirements for the length of time private record(s) of an Elected Official must be retained and the appropriate means of disposal at the end of its lifecycle. It is a best practice to develop a record retention and disposal schedule for your office to ensure that you have a list of all of the pi/phi that you have collected as well as knowing when you can delete such information.

Elected Officials that have collected pi/phi should destroy the sensitive information as soon as they no longer require it or the file is closed.

If an Elected Official no longer is running for office, the Elected Official may wish to transfer or share certain open files related to unresolved issues or cases where the constituent or organization is now represented by another Elected Official. If there are records of a sensitive nature or containing pi/phi, the Elected Official should get written consent from the individual before transferring the records.

In assessing what is the appropriate retention period and whether it is time to dispose of pi or phi, an Elected Official should consider the following points:

- Reviewing the purpose for having collected the personal information in the first place is generally helpful in assessing how long certain pi/phi should be retained.

- If pi/phi was used to make a decision about an individual, it should be retained for the legally required period of time – or other reasonable amount of time in the absence of legislative requirements – to allow the individual to access that information in order to understand, and possibly challenge, the basis for the decision (i.e., employment records that hold pi/phi).

- If retaining pi/phi any longer would result in a prejudice for the concerned individual, or increase the risk and exposure of potential data breaches, the Elected Official should consider safely disposing of it.

Securely disposing of personal information/personal health information

If an Elected Official has pi/phi in his or her control, he or she cannot simply throw it away in the trash. The Elected Official must find a way to securely dispose of it.

In instances where an Elected Official is planning a move, or is closing his/her doors, pi/phi should be securely transferred or safely disposed of.

There are a number of commonly accepted ways for Elected Official's to properly dispose of pi/phi depending on the form in which it is being stored. The goal is to irreversibly destroy the media which contains pi/phi so that this information cannot be reconstructed or recovered in any way. When going through the process of disposal, an Elected Official should also destroy all associated copies and backup files.

Types of personal information media storage

Information is mainly stored on two kinds of media:

- Hard copy: physical representations of data, such as paper. This includes, among other things, notes, memos, messages, correspondence, transaction records and reports.

- Electronic copy: information stored on electronic media, such as computer hard drives, copier and printer hard drives, removable solid drives including memory, disks and USB flash drives, mobile phones and magnetic tapes.

There are several ways in which pi/phi can be securely destroyed or removed by completely destroying the media, whether hard or electronic copy. It is a way to ensure that the information stored on it can never be recovered. This can be accomplished using a variety of methods including disintegration, incineration, pulverizing, shredding using a cross-shed shredder and melting.

Use of third parties

An Elected Official should assess the risks and benefits of destroying pi/phi on-site or off-site. If an Elected Official does not have appropriate tools to safely destroy sensitive information on-site, it may consider the services of a third-party contractor. In some cases, the sheer volume of the pi/phi to be disposed of can tip the balance towards using companies specialized in data destruction.

When considering using a third party to dispose of pi/phi an Elected Official should take into account the sensitive nature of the information and take steps to manage the risks accordingly.

An Elected Official should ensure that the third party contractor has verifiable credentials and can guarantee both a secure transfer of records from the Elected Official's office to their own destruction facility, and a secure destruction method that matches the media and information sensitivity.

If an Elected Official decides to contract out, he or she should keep in mind that he/she remains responsible for the information to be disposed of. Best practices when dealing with third parties include:

- Entering into a written contract with the contractor;
- Including privacy protection clauses in the contract to ensure the third party provides a level of protection that you are comfortable with; and
- Including monitoring and auditing clauses to ensure track record and quality control.

Putting it all together: Developing internal policies and procedures

In setting up policies and procedures, an Elected Official should consider the following checklist:

- ✓ Is information in the Elected Official's office periodically being reviewed to determine whether the purpose of the collection has been fulfilled? How often?
- ✓ Is there an inventory of what pi/phi is being retained, for which purpose and for how long?
- ✓ Have you developed a records retention and disposal schedule?
- ✓ Does pi/phi exist in multiple copies? Are there back-ups? If so, where are the copies and back-ups stored?
- ✓ When should the Elected Official dispose of the pi/phi ?
- ✓ How should the Elected Official dispose of pi/phi, copies and backups?
- ✓ What measures should be taken to ensure the equipment or devices used for storing the pi/phi (mobile phones, copiers, scanners, etc.) are properly disposed of, or sanitized?

- ✓ Is there a designated secure area for destroying documents?
- ✓ Is pi/phi being segregated and stored in a secure area with restricted access?

If you have questions regarding the security or disposal of pi/phi that is in your possession and control during your term, please feel free to contact the office of the Saskatchewan Information and Privacy Commissioner at:

Telephone: 306-787-8350
Toll Free Telephone (within Saskatchewan): 1-877-748-2298
Fax: 306-798-1603
Email: webmaster@oipc.sk.ca