

SASKATCHEWAN
OFFICE OF THE
INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT H-2007-001

SASKATCHEWAN HEALTH

Summary: Three individuals complained to the Commissioner that each received mail from branches of Saskatchewan Health (SK Health) in unsealed or improperly sealed envelopes. Each individual was concerned as the letters within those envelopes consisted of either the data subject's personal information or personal health information. Even though SK Health relies on Saskatchewan Property Management (SPM) to process some of its bulk mailings, the Commissioner found that this does not relieve SK Health of its obligation under section 16 of *The Health Information Protection Act* to protect personal health information. The Commissioner found, although there was no evidence of improper access to the personal information/personal health information contained within the improperly or unsealed envelopes, SK Health did not have adequate safeguards in place to protect personal information/personal health information externally processed for mailing by SPM.

Statutes Cited: *The Freedom of Information and Protection of Privacy Act*, [S.S. 1990-91, C. F-22.01 as amended] ss. 2(1)(d)(i), 24(1), 33(d); *The Health Information Protection Act*, [S.S. 1999, C. H-0.021, as amended] ss. 2(j), 2(m), 2(t)(i), 4(4)(g.1), 16, 18, 42(1)(c), 52(d)

Authorities Cited: OIPC, Investigation Reports H-2005-002, F-2007-001; OIPC Reports F-2004-006, F-2006-003, 2003-2004;

Office of the British Columbia Information and Privacy Commissioner, *Investigation Report F06-02*, available at http://www.oipcbc.org/orders/investigation_reports/InvestigationReportF06-02.pdf;

Information and Privacy Commissioner of Ontario, *Special Report to the Legislative Assembly of Ontario on the Disclosure of Personal Information by the Shared Services Bureau of Management Board Secretariat, and the Ministry of Finance*, (December 16, 2004); available at http://www.ipc.on.ca/images/Resources/up-pc040077_e.pdf;

Privacy Commissioner of Canada, *PIPEDA Case Summaries #197 & #154* available at http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030801_02_e.asp; and

Prince Edward Island Information and Privacy Commissioner, *Order PP-04-003*; available at <http://www.assembly.pe.ca/foipp/PP-04-003.pdf>

**Other
Sources
Cited:**

OIPC *Annual Report 2005-2006*; Saskatchewan FOIP FOLIO, December 2005, January 2006, and September 2006; OIPC, *2006-2009 Business Plan*; OIPC, *Letter to the Speaker on Bill 61, The Vital Statistics Act 2007*, (May 9, 2007); available at <http://www.oipc.sk.ca/webdocs/vitalstats.pdf>;

Graham W.S. Scott et al., *The Personal Health Information Protection Act – Implementing Best Privacy Practices*, (Canada: Butterworth, 2005);

Elizabeth Wilcox and Alberta Queen's Printer, *The Annotated Alberta Freedom of Information and Protection of Privacy Act*, (2005, Alberta Queen's Printer, Edmonton);

COACH Guidelines for the Protection of Health Information; Saskatchewan Health, *Drug Plan & Extended Benefits Branch*, available at http://www.health.gov.sk.ca/ph_br_drug_plan_ext_ben.html;

Saskatchewan Property Management, *2005 – 2006 Provincial Budget Performance Plan*, Saskatchewan Property Management; available at: http://www.spm.gov.sk.ca/docs/spm_performance_plan_2005-06.pdf;

Saskatchewan Property Management, *About Us*; available at http://www.spm.gov.sk.ca/about_us.cfm; Saskatchewan Property Management, *Mail Services*, available at: http://www.spm.gov.sk.ca/services_mail.cfm;

Special Report from Buyers Laboratory Inc dated January 2003 titled *A Buyers Guide to Mailing Machines*; available at <http://www.addtronics.net/mailing/bli.pdf>;

Saskatchewan Labour, *Occupational Health and Safety Division, Inspections Appendix*, (October 2002); available at http://worksafesask.com/files/sask_labour/inspections3.pdf;

Canadian Patient Safety Institute, *Canadian Root Cause Analysis Framework – A tool for identifying and addressing the root cause of critical incidents in healthcare*, (March 2006); available at http://www.patientsafetyinstitute.ca/uploadedFiles/Resources/RCA_March06.pdf;

Saskatchewan Labour, Occupational Health and Safety, *Accident Investigations – A Guide for Committees and Representatives*, (October 2002); available at <http://www.labour.gov.sk.ca/safety/accidentinvestigations/AccidentInvestigationspart1.pdf>;

What to do when faced with a Privacy Breach Guidelines for the Health Sector, (Ontario Information and Privacy Commissioner); available at <http://www.ipc.on.ca/images/Resources/up-3hprivbreach.pdf>;

Government of Alberta, *Managing Contracts under the FOIP Act, A Guide for Government of Alberta Contract Managers and FOIP Coordinators, Discussion Draft*, (September 2005); available at <http://foip.gov.ab.ca/resources/publications/pdf/contractmanager.pdf>; and

Setting Up A Complaint-Handling Process, (December 2004); available at <http://www.psp.gov.ab.ca/resources/pdf/ComplaintHandling.pdf>.

I. BACKGROUND

- [1] Our office received complaints from three individuals alleging that he/she received mail from Saskatchewan Health (SK Health or the Department) in unsealed or improperly sealed envelopes. In addition to these complaints, our office received an envelope from the Department intended for a third party that required resealing by us prior to mailing.

First complainant

- [2] The original complainant claimed that on January 26, 2004 he received a letter on SK Health letterhead dated January 16, 2004 in an unsealed envelope.
- [3] This letter originated from the Department's Drug Plan and Extended Benefits (DPEB) Branch. SK Health's website describes the branch as follows:

The Drug Plan and Extended Benefits Branch provides benefits to the eligible Saskatchewan population by promoting cost-effective drug therapy and extended benefits, subsidizing qualifying residents and supporting the use of a claims database.¹

Second complainant

- [4] The second complainant notified us of her concerns by way of letter dated April 11, 2005. She alleged that she received birth certificates from SK Health's Health Registrations and Vital Statistics (HRVS) Branch in an unsealed envelope.
- [5] SK Health's website provides the following background with respect to services provided by Health Registration and Vital Statistics:

Health Registration registers new residents of the province for coverage and maintains the registry of all residents who are eligible for benefits.

The branch also issues a health services card to individuals once you are approved for benefits. The card is a valuable personal identification document and is required for presentation when you need health services.

...

¹ Saskatchewan Health, Drug Plan & Extended Benefits Branch, available at http://www.health.gov.sk.ca/ph_br_drug_plan_ext_ben.html

The Vital Statistics:

- *administers and maintains a province-wide system for registering births, deaths, marriages, stillbirths, divorces, adoptions and changes of name that occur in Saskatchewan.*²
- ...

Third complainant

- [6] Our office notified the Department on September 7, 2005 of an unsealed envelope received by a third complainant at her home on August 3, 2005.
- [7] As our office inspected all three of the envelopes in question, we are satisfied that all three complainants' concerns are well-founded.

Last incident

- [8] In our dealings with SK Health on another matter, as the Department sought to provide information to a number of individuals who wished to remain anonymous, it provided letters to us in sealed envelopes which we would in turn address and mail to those individuals only known to us. When SK Health couriered the letters to us on May 25, 2005, however, one of the 26 letters arrived at our office unsealed.

II. AUTHORITY TO INVESTIGATE PRIVACY COMPLAINTS

- [9] I undertook this investigation pursuant to sections 42(1)(c), and 52(d) of *The Health Information Protection Act*³ (HIPA) and section 33(d) of *The Freedom of Information and Protection of Privacy Act*⁴ (FOIP).
- [10] Section 42(1)(c) of HIPA is reproduced below:

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

...

(c) *the person believes that there has been a contravention of this Act.*

² Saskatchewan Health, *Health Registration and Vital Statistics*, available at http://www.health.gov.sk.ca/ph_br_hrvsb.html

³ *The Health Information Protection Act*, S.S. 1999, C. H-0.021, as am. (hereinafter HIPA)

⁴ *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, C. F-22.01, as am. (hereinafter FOIP)

[11] Section 52(d) of HIPA reads as follows:

52 *The commissioner may:*

...

(d) from time to time, carry out investigations with respect to personal health information in the custody or control of trustees to ensure compliance with this Act.

[12] Section 33(d) of FOIP reads as follows:

33 *The commissioner may:*

...

(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.

III. OIPC INVESTIGATIVE PROCESS

[13] To provide guidance to government institutions, local authorities, and trustees on how to respond when learning of a potential privacy breach, in our January 2006 issue of our FOIP FOLIO,⁵ I offered the following:

If you work for a government institution, local authority, or health trustee and have learned of a possible privacy breach, we would recommend that you notify your immediate supervisor and/or Privacy Officer/FOIP Coordinator or follow the internal reporting requirements prescribed by your organization's privacy policy and procedures.

Once in the hands of the appropriate personnel, we recommend that the public body take the following action:

- *Conduct an internal investigation:*
 - *Identify the scope of the breach;*
 - *Take immediate corrective action and contain damage;*
 - *Review existing policies, procedures, safeguards, etc. to see if adequate; and*
 - *Report findings and take necessary and appropriate action to prevent future breaches.*

[14] Our office notified SK Health of our receipt of the first complaint by way of letter dated June 2, 2004. We provided notification to SK Health of our receipt of the second

⁵ *Saskatchewan FOIP FOLIO*, (January 2006), at 4; available at <http://www.oipc.sk.ca/FOIPFOLIO/January2006.pdf>

complaint by way of letter dated May 11, 2005, and of the third and last incident via electronic mail (e-mail) on September 7, 2005 and May 25, 2005 respectively.

[15] This investigation involves two government departments: SK Health and Saskatchewan Property Management (SPM). During the course of this investigation, SPM underwent a name change as follows: “*The Department of Property Management will replace the Saskatchewan Property Management Corporation (SPMC) as of April 1, 2005.*”⁶ As it was unclear which department improperly sealed the envelopes in question, we initiated discussions with both.

[16] During the course of this investigation, the following also occurred:

1. SK Health and SPM discussed the aforementioned incidents on numerous occasions.
2. SK Health advised us that it immediately offers “*complainants involved in a privacy breach with a sincere apology.*”

The Department offered both a verbal and written apology to the first complainant. The complainant was dissatisfied however as, in his opinion, the Department did not provide enough details as to the steps taken to prevent a similar occurrence in the future.

In terms of the second complainant, SK Health submits that its Director, Health Registration and Vital Statistics, recalls offering an apology to this individual during a phone conversation in the year 2005. Though the complaint informs us that she talked to a number of individuals from the Department around the time of the incident, she does not recall receiving a verbal apology; but is certain she did not receive a written apology from the Department.

The third complainant received a written apology from the Department via email.

3. SK Health informed us in writing on July 15, 2004 that it conducted a review of its mail handling procedures.

⁶ Saskatchewan Property Management, 2005 – 2006 Provincial Budget Performance Plan, Saskatchewan Property Management, at 2; available at: http://www.spm.gov.sk.ca/docs/spm_performance_plan_2005-06.pdf

4. On March 9, 2005, we interviewed the Director, System and Client Support Services, SK Health, as the complainant first raised his concerns with this individual. The Director explained the process for preparing envelopes prior to delivering to SPM includes keeping the flaps open and binding with elastics. This is a manual process. If the flap is not up, the machine may not grab and seal properly.
5. We met with representatives from SK Health on July 26, 2005. Representatives from the Department included its Director, Strategic Planning and Information Policy and Privacy Officer; Executive Secretary; Executive Director; and Senior Policy Analyst to discuss the complaints of unsealed envelopes.

The Senior Policy Analyst provided further detail regarding the mail handling process. She explained that the mail is generally unsealed when delivered to SPM. At SPM, a machine will seal the envelopes and affix postage. When the envelopes fall out of the machine (into a bucket), they are stacked on top of each other so the weight will help the seal set. Then, an employee will perform a visual check for unsealed envelopes and if necessary, reseal manually (re-wet) or even tape as a last resort. She explained that envelopes may not seal if the flaps are down when entering the machine, so staff are instructed to ensure flaps are open prior to feeding into the machine.

6. SK Health sent a letter dated November 3, 2005 to its Senior Administrative Support staff requesting revisions to Department mail service practices, including eliminating the use of glue stick to seal mail, and requiring personnel to seal all small mail-outs containing personal health information prior to forwarding to SPM.
7. Though in a letter dated November 3, 2005, SK Health noted its satisfaction with SPM's current mail services processes, the Department nonetheless requested that SPM Mail Services Branch consider a review of its processes to decrease the potential for envelopes arriving at intended destinations unsealed.
8. We attended on site at SPM's main mailroom (Central Sort) at 110 Henderson Drive in Regina on November 30, 2005 to observe the processing of mail. After the

machine sealed a stack of envelopes, upon a quick visual check, the lone handler pulled two unsealed envelope from the stack, resealed them, and then slid the resealed envelopes back into the stack.

9. SK Health advised us that on April 4, 2007, a Senior Policy Analyst from SK Health toured this facility. This tour included a demonstration of the mail-sealing machine and sealing process, and identification of the precautionary measures followed by SPM staff to ensure appropriate sealing.

IV. ISSUES

1. **Was the information in question in all three incidents “personal information” as defined by section 24(1) of *The Freedom of Information and Protection of Privacy Act* or “personal health information” as defined by section 2(m) of *The Health Information Protection Act*?**
2. **Which government institution, SK Health or SPM, is responsible to ensure proper sealing of confidential mail prior to pick up by Canada Post?**
3. **Does SK Health have adequate mechanisms in place to ensure personal health information is protected when mailed?**

V. DISCUSSION OF THE ISSUES

1. **Was the information in question in all three incidents “personal information” as defined by section 24(1) of *The Freedom of Information and Protection of Privacy Act* or “personal health information” as defined by section 2(m) of *The Health Information Protection Act*?**

[17] SK Health and SPM are “*government institutions*” for the purposes of FOIP⁷ and “*trustees*” as defined by HIPA⁸.

[18] SK Health elaborated as follows on what services provided by these two divisions (DPEB & HRVS) would require sending the data subject’s personal information/personal health information through the mail:

⁷ Section 2(1)(d)(i) of FOIP: “*government institution*” means, subject to subsection (2): (i) the office of Executive Council or any department, secretariat or other similar agency of the executive government of Saskatchewan...”

⁸ Section 2(t)(i) of HIPA: “*trustee*” means any of the following that have custody or control of personal health information: (i) a government institution...”

Drug Plan and Extended Benefits

The bulk of the letters sent from the Drug Plan and Extended Benefits Branch are letters confirming benefits provided through programs offered by this Branch, including the Special Support, Exception Drug Status, and Oxygen programs. Letters to individuals and physicians requesting additional information are also sent.

Health Registration

1) Health Card Applications

- a) The application form completed by the applicant contains personal information pertaining to the applicant and his/her family. Required information includes name, date of birth, address and telephone. If the application form is incomplete, it may be returned by mail to the applicant for completion and re-submission.*
- b) Photocopies of two personal identification documents are required for each adult named on the application. Acceptable documents include driver's licence, birth certificate, SIN/Treaty/Canadian Citizenship card and health card from the last province of residence. If the applicant sends in an original document, it is returned to the applicant by mail via S.P.M.*

Mail associated with (a) and (b) is packaged for delivery by the branch and is turned over to S.P.M. for metering, sealing and transfer to Canada Post.

2) Health Cards

There are two types of health cards issued by the Department, the plastic health card, and the paper supplementary health card. These cards are issued by ISM [Information Systems Management Corporation] at their Regina production facility.

- a) The plastic Health Services Card is issued to each eligible resident of the province. The personal information contained on the card is name, date of birth, gender and Health Services Number. ISM acquires all necessary blank stock (e.g. cards, envelopes), personalizes the cards, prepares the cards for mailing (i.e. package and seal the envelopes), and provides the envelopes to Canada Post for delivery.*
- b) The paper Supplementary Health Card is issued only to persons who meet certain income thresholds. The card lists all persons in the family unit who are eligible for supplementary coverage. The personal information for each family member contained on the card is name, date of birth, gender, benefits type/level and Health Services Number. These cards are pressure sealed. ISM acquires the blank card stock, personalizes the cards, folds and seals the cards, and provides the cards to Canada Post for delivery.*

3) Other

Some correspondence between the Branch and the registrant may contain personal/personal health information. Such mail is packaged for delivery by the branch and provided to S.P.M. for metering, sealing and transfer to Canada Post.

Vital Statistics

1) Certificate/Change of Name Applications

The application form completed by the applicant to obtain a vital event certificate (birth/marriage/death) or a legal change of name contains personal information pertaining to the applicant and his/her family. Required information may include name, address, date of birth/marriage/death and, parents' names. The application may also contain credit card information (i.e. issuer, card number, and expiry date) if payment is being made by credit card. If the application form is incomplete, it may be returned by mail to the applicant for completion and re-submission. The applications being returned are packaged for delivery by the branch and are provided to S.P.M. for metering, sealing and transfer to Canada Post.

2) Certificates

The personal information contained on the vital event certificates includes name, gender, date of birth/marriage/death, parents' names, medical cause of death, and the event registration number. The cash register or credit card receipt confirming payment processing is included with the certificate. The certificates are packaged for delivery by the Branch and are provided to S.P.M. for metering, sealing and transfer to Canada Post.

3) Other

Some correspondence between the branch and the registrant may contain personal/personal health information. Such mail is packaged for delivery by the Branch and provided to S.P.M. for metering, sealing and transfer to Canada Post.

- [19] The first complainant's envelope contained the complainant's address, health services number, and details of his coverage under the drug plan including the individual's share of drug costs for each six month benefit period.
- [20] The third complainant received information similar to that outlined above from the same branch (DPEB) of the Department.
- [21] The envelope, however, subject of the complaint from the second complainant contained two small birth certificates from Vital Statistics (HRVS) for the complainant and her spouse. The information contained on each certificate included each data subject's name [surname and given names(s)], date of birth, gender, place of birth, registration date and number, and certificate issue date. SK Health indicated that no payment receipt would have been included in the envelope as the method of payment for these certificates was by personal cheque.

[22] The fourth envelope contained a letter from SK Health that responded to a breach of privacy complaint that involved the Prevention Program for Cervical Cancer.

[23] I find that the envelopes contain personal information and personal health information as defined by section 24 of FOIP and 2(m) of HIPA.

2. Which government institution, SK Health or SPM, is responsible to ensure proper sealing of confidential mail prior to pick up by Canada Post?

[24] SK Health responded as follows to our questions (bolded):

What is Saskatchewan Health's arrangement with Saskatchewan Property Management (SPM) regarding confidential mail-outs?

*Currently, six Branches [of SK Health] have **a direct arrangement** with SPM regarding confidential bulk mail-outs. **Arrangements include established agreements** for SPM to process mail (fold, stuff, seal, and meter) for delivery to Canada Post. ...On occasion, two additional Branches forward larger mail outs to the Saskatchewan Health mailroom, which are then picked up by SPM for sealing and distribution.*

Does each Saskatchewan Health Branch have its own mail-sealing machine?

Only one Branch, the Provincial Laboratory Branch...

Or is all mail that is sent directly from Saskatchewan Health sealed individually by staff?

Mail sent directly from Saskatchewan Health is sealed through various methods, including individually, by designated Branch employees, through the Saskatchewan Health mailroom staff, by ISM, or by SPM.

[Emphasis added]

[25] When asked about the arrangement between the two departments, SK Health reported the following:

A formal, written agreement between Saskatchewan Health and S.P.M. does not exist.... S.P.M. is a government department, which provides mail-handling services for all government departments; none of which have formal agreements in place. The Mail Services Branch of S.P.M. has an objective to offer economies by centralizing mail handling resources without restricting delivery standards.

[26] For more information on the services provided by SPM, I canvassed various websites as follows:

SPM provides mail handling services for government departments, most government boards, commissions, corporations and authorized public agencies to

achieve economies of scale through centralization of mail handling resources. Mail is handled through 14 provincial centres and includes pick-up, sorting, delivery of Canada Post mail, metering of outgoing mail, addressing and stuffing mail, and offering volume discounts for parcel, priority courier and bulk mailings. Inter-office mail, using reusable envelopes, is co-ordinated between Regina and 26 centres, as an alternative to Canada Post.⁹

Saskatchewan Property Management is comprised of four divisions: Accommodation Services, Commercial Services, Corporate Support Services, and Information Technology with a staff complement of approximately 828 full-time equivalent employees. The organization generates approximately \$200M annually in revenues, which recover the cost of delivering the services.

SPM is mandated to provide accommodation and support services to government departments, Crown Corporations, boards, agencies and commissions. The organization also provides these services to other levels of government and to various non-governmental organizations. We operate under our own legislation.¹⁰

Mail Services provides mail and related services for all government departments and agencies. The agency handles approximately 23.9 million pieces of government mail per year and maintains quick, reliable delivery to government offices throughout the province.

Mail Services operates central mailrooms in 14 urban centres and provides centralized mail handling staff and equipment, including daily pick-up and delivery. Mail Services also offers overnight delivery to 26 centres as well as a courier service in Regina.¹¹

- [27] SPM provides a service for SK Health. Does this, however, make SPM responsible if a privacy breach occurs because it improperly sealed an envelope on behalf of SK Health?
- [28] FOIP vests responsibility in government institutions for personal information in its possession or control. HIPA requires similarly that trustees safeguard personal health information in its custody or control.¹²
- [29] In my last Annual Report, I explained that the word “custody” in HIPA is to be understood as “physical possession”.¹³ FOIP, however, uses the term “possession” in the

⁹ Saskatchewan Property Management, 2005 – 2006 Provincial Budget Performance Plan, Saskatchewan Property Management, at 4; available at: http://www.spm.gov.sk.ca/docs/spm_performance_plan_2005-06.pdf

¹⁰ Saskatchewan Property Management website, *About Us*; available at http://www.spm.gov.sk.ca/about_us.cfm

¹¹ Saskatchewan Property Management, *Mail Services*, available at: http://www.spm.gov.sk.ca/services_mail.cfm

¹² HIPA, s. 16: “...a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will...”

place of “custody”. I find that these two terms are interchangeable as they have the same connotation.

[30] In Report F-2004-006 [58], I determined the following:

*I take the foregoing underlined passage to be a recognition that possession and control are different things. Otherwise, there would be no need to have both words. It is therefore conceivable that a government institution might have possession but not control of a record or that it might have control of a record but not possession.*¹⁴

[31] *The Annotated Alberta Freedom of Information and Protection of Privacy Act* offers further insight into the applicability of the terms “custody” and “control”:

*... “Custody” refers to the physical possession of a record, while **“control” refers to the authority of a public body to manage, even partially, what is done with a record.** For example, the right to demand possession of a record, or to authorize or forbid access to a record, points to a public body having control of a record (Orders 2000-003 [32], F2002-014 [12]).*¹⁵

[Emphasis added]

[32] I find that given the information available to us, SK Health retains the authority to manage what is done with the personal information/personal health information when the stuffed envelopes are delivered to SPM for sealing.

[33] It appears that to the extent that SPM processes SK Health’s personal health information for mailing, SPM is functioning as an information management service provider as contemplated by section 18 of HIPA. The provision is reproduced below:

18(1) A trustee may provide personal health information to an information management service provider:

*(a) for the purpose of having the information management service provider **process, store, archive or destroy the personal health information for the trustee;***

...

¹³ Office of the Saskatchewan Information and Privacy Commissioner, *2005-2006 Annual Report*, at 52; available at <http://www.oipc.sk.ca/Reports/AnnualReport05-06.pdf>

¹⁴ Office of the Saskatchewan Information and Privacy Commissioner, *Report F-2004-006*, at [58]; available at <http://www.oipc.sk.ca/Reports/2004-006.pdf>.

¹⁵ Elizabeth Wilcox and Alberta Queen’s Printer, *The Annotated Alberta Freedom of Information and Protection of Privacy Act*, (2005, Alberta Queen’s Printer, Edmonton) at 5-6-3.

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

...

(5) *If a trustee is also an information management service provider and has received personal health information from another trustee in accordance with subsection (1), the trustee receiving the information is deemed to be an information management service provider for the purposes of that personal health information and does not have any of the rights and duties of a trustee with respect to that information.*

[Emphasis added]

[34] Section 2(j) of HIPA defines “*information management services provider*” as follows:

a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf.

[35] In our Investigation Report H-2005-002, I considered whether or not the Saskatchewan Cancer Agency was acting as an information management service provider when accessing personal health information for different functions. The portions of that Report relevant to this matter are as follows:

To qualify as an information management service provider, an assessment must be done, apart from any contractual description or label, to see if the definition or elements of that definition apply.

The question of an information management services provider is important since the scheme of HIPA is to vest in a given trustee clear responsibility for protecting the privacy of a woman and the confidentiality of her personal health information.¹⁶

...

After considering these materials, I take the intention of the Saskatchewan Legislative Assembly to be that the conveyance of personal health information to an information management services provider would be a ‘use’ and not a ‘disclosure’ for purposes of HIPA.¹⁷

¹⁶ Office of the Saskatchewan Information and Privacy Commissioner, *Investigation Report H-2005-002*, at 141; available at www.oipc.sk.ca under *Reports*.

¹⁷ *Ibid*, at 143.

[36] Even in the absence of a contractual agreement between the two departments, I find that SPM is acting in an information management service provider role when it processes personal health information for mailing on SK Health's behalf and at its request. Accordingly, I find that SK Health retains responsibility for safeguarding personal health information when it is processed for mailing by SPM.

3. Does SK Health have adequate mechanisms in place to ensure personal health information is protected when mailed?

[37] All of HIPA applies to SK Health for services provided through its Drug Plan and Extended Benefits Branch. Three parts of HIPA, however, do not apply to personal health information "*obtained for purposes of The Vital Statistics Act, 1995 or any former Vital Statistics Act*".¹⁸ Part III of HIPA does apply, though, to both divisions (DPEB & HRVS) of SK Health. Section 16 in this part requires that the trustee have the following in place:

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

- (a) protect the integrity, accuracy and confidentiality of the information;*
- (b) protect against any reasonably anticipated:*
 - (i) threat or hazard to the security or integrity of the information;*
 - (ii) loss of the information; or*
 - (iii) unauthorized access to use, disclosure or modification of the information; and*
- (c) otherwise ensure compliance with this Act by its employees.*

[38] As is evident from this investigation and due to the sheer volume of mail processed, I find that it is reasonable to anticipate that the odd envelope may continue to be improperly sealed; thus allowing individuals without the requisite authorization to access the contents. Therefore appropriate safeguards must be adopted to mitigate the chances of this occurring.

[39] In our Investigation Report H-2005-002, I offered the following with respect to what safeguards are required to adequately protect personal health information:

¹⁸ HIPA, section 4(4)(g.1)

HIPA does not particularize the kinds of safeguards required to discharge the section 16 obligation.

Our office views Guidelines for the Protection of Health Information produced by Canada's Health Informatics Association as the relevant standard or best practice for Saskatchewan trustee organizations. In addition, there is much useful information in the Privacy and Security Rules published under the United States Health Insurance Portability and Accountability Act of 1996.

...

To discharge its obligation under section 16 of HIPA, I find that a trustee must address three different kinds of safeguards: (1) administrative; (2) technical and (3) physical.

In addition to the contractual arrangements made with other trustees for purposes of PPCC or information management services provided by the Agency to the two large health regions, the Agency has also developed a number of safeguards to protect the personal health information under its control.¹⁹

[40] The Guidelines²⁰ noted above stress that classifying health information once collected is necessary “...in order to ensure that protection levels are commensurate with the sensitivity of the information being protected...” Classification is defined in the same resource as “a system for determining the sensitivity of personal health information and for establishing priorities for information security and privacy protection.”²¹

[41] It is unclear if SK Health has undertaken efforts to classify its personal information/personal health information holdings. However, in terms of the sensitivity of vital statistics information, my May 9, 2007 commentary on Bill 61, *The Vital Statistics Act, 2007*, tabled in the Legislative Assembly offered the following for consideration:

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”. 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

¹⁹ *Supra*, note 16 at 97

²⁰ COACH - Canada’s Health Informatics Association, *COACH Guidelines for the Protection of Health Information* (Coach, 2004) at 62.

²¹ *Ibid*, at 77.

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.

...

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 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.

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.²²

[Emphasis added]

[42] As the information sent through the mail by SK Health includes personal health information and personal information used to establish identity, I find that those data elements constitute sensitive information. Though there is no evidence that anyone other than the intended recipient was able to view the information contained within each improperly or unsealed envelope, we are still concerned as the potential existed and if the cause is not identified, then the threat continues.

[43] I must now make a determination as to whether the protections put in place by SK Health are commensurate with the sensitivity of the information requiring protection.

²² Office of the Saskatchewan Information and Privacy Commissioner, *Letter to the Speaker on Bill 61, The Vital Statistics Act 2007*, (May 9, 2007); available at <http://www.oipc.sk.ca/webdocs/vitalstats.pdf>

[44] Section 16 of HIPA does not require a standard of perfection but one of reasonableness. In Investigation Report F06-02, a Portfolio Officer with British Columbia's Office of the Information and Privacy Commissioner applied the 'standard of reasonableness'. The relevant excerpts are reproduced as follows:

[2] *Public bodies in British Columbia are under a statutory duty to protect the personal information in their custody or under their control. Section 30 of FIPPA sets out the legal requirement:*

Protection of personal information

30 *A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*

...

[31] ***3.6 Analysis of Data Sensitivity and Protective Measures*** — *Section 30 of FIPPA requires public bodies to take reasonable measures to protect information under their custody or control. In Investigation Report F06-01, Commissioner Loukidelis said this about s. 30:*

[49] *By imposing a reasonableness standard in s. 30, the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one's personal best. **The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable" does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.***

[50] *The reasonableness standard in s. 30 is also not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.*

[32] ***The reasonableness of security measures will depend on the sensitivity of the information.*** *As the Commissioner also noted in Investigation Report F06-01:*

[52] *The sensitivity of the personal information at stake is a commonly cited, and important, consideration. For example, a computer disk or paper file containing the names of a local government's employees who are scheduled to attend a conference or take upcoming vacation does not call*

*for the same protective measures as a disk containing the medical files of those employees.*²³

[Emphasis added]

[45] I am of the same view. Accordingly, I must determine if I agree with SK Health's self-assessment that it currently has adequate processes in place as is evident by the following:

*Given the amount of mail that SPM handles in one year (24 million pieces), of which 110,000 health cards and 68,000 certificates originate from the Health Registration and Vital Statistics Branch and 100,000 pieces originate from the Drug Plan and Extended Benefits Branch, **our Department is reasonably satisfied with the current practices and processes.***

[Emphasis added]

[46] I find the argument that since SPM processes such a massive quantity of mail, it is acceptable for a relatively small percentage of envelopes processed to leave the mailroom improperly sealed unpersuasive for the risks articulated earlier.

[47] Nonetheless, the question is whether SK Health has adopted reasonable safeguards in the circumstances. To make this determination, I must firstly identify what safeguards SK Health had in place when each of the four complaints surfaced and then consider what improvements were made over the course of this investigation.

[48] SK Health indicated to us that it safeguards confidential mail as follows:

Safeguards include sealing mail through SPM, within Branches or within the Saskatchewan Health mailroom (with sponge sealers, tape guns, wet cloth or glue sticks), with a mail-sealing machine (1 Branch), and with a heat-sealing process (1 Branch through ISM). Additional processes include securing envelopes with packing tape and thoroughly reviewing the envelope to ensure secure sealing.

[49] During a meeting involving our office and representatives from SK Health on July 26, 2005, after inspection of the two envelopes forwarded to our office by the first two complainants, SK Health indicated that the sealing was done by SPM, not SK Health. The third complaint did not surface until sometime after this meeting so SK Health did not have opportunity to inspect the envelope subject to that complaint. In the case of the

²³ Office of the British Columbia Information and Privacy Commissioner, *Investigation Report F06-02* at 2, 7 & 8, available at http://www.oipcbc.org/orders/investigation_reports/InvestigationReportF06-02.pdf;

last incident, because we provided SK Health notice the same day the envelope was received, SK Health was able to immediately identify the reason why the envelope did not seal properly even without inspecting it. We were advised a glue stick was used and appears to have contributed to the seal failing.

[50] On March 12, 2005, we asked SK Health what procedures are in place to minimize or eliminate the possibility of unsealed envelopes being sent out. In response, the following was provided:

[SK Health's Executive Secretary] learned from the 3085 Albert Street that the operator there does visual checks through the stuffing, sealing and metering process to ensure envelopes are okay for mailing. [SK Health's Director, System and Client Support Services] learned from 3211 Albert Street that the operator checks elastic bound groupings of letters to ensure all envelopes are flapped open before going into the mail machines, and then checks that [sic] are sealed when coming out of the machine. This operator did mention on occasion an envelope that has been sealed will open after the fact when bent.

[51] In terms of its mail services units, SPM offered the following: *"All three units at Central sort and 3085 Albert are Neopost SM 94 and at 3211 it's a Pitney_Bowes 5600"*. Further, SK Health advised us that the Director of Mail Services *"noted that the S.P.M. Mail Services Branch implements mail service units, which are the best that the industry has to offer"*.

[52] SPM's Director of Mail Services, SK Health's main contact who is responsible for handling mail services issues including privacy and service failures, provided the following when asked for more specifics about the machines used and industry standards:

- 1. Our RFP [request for proposal] does not specify a particular mode [sic]. – it asks for a system which includes lo med and hi volume machines – we currently have 70 units areound [sic] the prov [sic] All three suppliers will be asked.*
- 2. Like cars each machine has a capacity to handle some better than others – the only way to determine is to try out the envelopes on the actual units. Glue is the big issue – and age of the envelope is a close second – paper gets brittle – glue develops a skin from air moisture*
- 3. Our Hi volume machines are filled several times daily and applicators are cleaned then The best indicator of need to clean is if the envelopes do not seal – then a cleaning is necessary. **Manufacture specs on our ancient units have***

***long since disappeared.** Our new units will be ink jet technology since Canada Post requires bar coding*

[Emphasis added]

[53] On July 13, 2006, SPM's FOI, Privacy, and Legislative Officer verified that all the machines in use as of that date had been used over the past several years. However, this changed in January 2007. SK Health reported that SPM replaced the mail-sealing unit which seals mail from SK Health, with a DM 1000 Pitney Bowes sealer. SK Health asserts that the new machine has a 99.99% success rate, and is also more mechanized than previous machines. In its recent correspondence to our office, SK Health elaborated, "[t]his increased mechanization decreases the potential for human error in sealing. In addition, the new machine applies pressure on each envelope, which helps to seal each envelope more effectively than the previous machine."

[54] Based on what was submitted to us and our own research,²⁴ I am unclear as to how SK Health concluded "*that the Mail Services processes currently in place meet our needs and industry standards*"²⁵ especially as this conclusion was reached prior to the purchase of the new equipment in January 2007.

[55] Our office also inquired further into the envelopes used by SK Health including, inter alia, possible contributors to sealant degradation. In response to the questions listed below (bold), SK Health offered the following responses:

Do you have a way of tracking when envelopes were purchased?

Branches reported maintaining copies of SPM invoices, receiving reports, purchase orders, packing slips, and order forms for envelopes ordered....

Can you confirm that all Saskatchewan Health envelopes are purchased from SPM?

The majority of Saskatchewan Health envelopes are purchased from SPM. However, some Saskatchewan Health envelopes are purchased from Supreme X (1 Branch), Grand and Toy (1 Branch), or other private suppliers.

...

Do you have a maximum shelf-life for your envelopes?

Saskatchewan Health Branches typically maintain envelopes for two months to one year.

²⁴ Inter alia, we reviewed a Special Report from Buyers Laboratory Inc dated January 2003 titled *A Buyers Guide to Mailing Machines* which compares different makes and models including the Neopost SM94; available at <http://www.addtronics.net/mailing/bli.pdf>.

²⁵ SK Health provided us with a copy of the letter it provided to SPM dated November 3, 2005.

- [56] Neither department provided copies of any policies, procedures, guidelines or standards that could be relied upon when making purchasing decisions with respect to what products/materials (i.e. envelopes) are best to buy.
- [57] SK Health indicated to us that SPM takes precautionary measures included inspecting and examining sealed mail to ensure appropriate sealing. As these practices were in place during the time that the three envelopes were improperly sealed, this reassurance is unpersuasive. SPM processes a huge volume of mail on a daily basis, which increases the potential for human or technical error or both. Implementation of checking procedures at several stages would increase the likelihood that if a seal fails, it would be discovered. The cause of the problem, however, would still have to be determined.
- [58] No clear explanation has been offered as to why each of the three envelopes did not seal properly. Replacing the mail sealing machine may remedy the problem; however, without knowing if the machine was the problem, this measure alone does not alleviate our concerns.
- [59] One way to evaluate the reliability of a system is to audit²⁶ it. Ontario's Information and Privacy Commissioner recommended that the Management Board Secretariat initiate a comprehensive and independent end-to-end audit of its Shared Services Bureau's functions, operations and privacy practices involving the handling of personal information in response to a breach involving a mass mail-out of third party personal information.²⁷
- [60] Sample questions to ask in this type of assessment include: (1) Did the equipment involved meet current codes, specifications and regulations? (2) Was there a maintenance program in place to maintain the equipment involved? (3) If previous inspections pointed to equipment problems, what corrective action(s) were taken and were they effective? For a better understanding of where systems may break down, a workflow diagram or

²⁶ An audit is a systematic, detailed, professional review of the entire system. An audit looks at all parts of the system and how those parts work together.

²⁷ Information and Privacy Commissioner of Ontario, *Special Report to the Legislative Assembly of Ontario on the Disclosure of Personal Information by the Shared Services Bureau of Management Board Secretariat, and the Ministry of Finance*, (December 16, 2004); available at http://www.ipc.on.ca/images/Resources/up-pc040077_e.pdf.

analysis could prove useful as “[w]orkflow diagrams and production flowcharts provide a “bird’s eye view” of how work flows from area to area....”²⁸

[61] A more reactive approach to determining a system’s failings is to conduct a root cause analysis after learning of an incident. In one document, root cause analysis is defined as:

A Root Cause Analysis is an intensive assessment conducted to prevent recurrence of an Occurrence by identifying the reason(s) underlying an undesirable condition or problem in the system. Characteristics of a Root Cause Analysis:

1. *The analysis focuses on systems and processes, not individual performance;*
2. *The analysis starts with the apparent cause(s) of the Occurrence and progresses to identification of reasons for any undesirable conditions or problems...*
3. *The analysis repeatedly digs deeper by asking why questions until no additional logical answer can be identified; and*
4. *The analysis identifies changes that could be made in systems and processes... that would improve the level of performance and reduce the risk of a particular serious adverse occurrence occurring in the future.*²⁹

[62] Though a process for investigating an accident or dangerous occurrence, the following is nonetheless a useful starting point to develop a process for determining the root cause of a privacy incident:

1. *Find out what caused the incident (immediate events leading up to the incident).*
2. *Find out what contributed to the incident (such as unsafe activities and conditions).*
3. *Find out what root causes set the stage (such as defective policies, procedures or attitudes).*
4. *Find ways to prevent a similar incident.*

...

Factors to think about might include:

- *inadequate planning, training, orientation, or supervision*
- *poorly designed work areas or job procedures*

²⁸ Follows a process from start to finish of identifying problems with systems. This can be accomplished by observing workers while at work and breaking down their actions into individual tasks. Problems may be noted at any stage. Saskatchewan Labour, *Occupational Health and Safety Division, Inspections Appendix*, (October 2002) at 89; available at http://worksafesask.com/files/sask_labour/inspections3.pdf.

²⁹ Canadian Patient Safety Institute, *Canadian Root Cause Analysis Framework – A tool for identifying and addressing the root cause of critical incidents in healthcare*, (March 2006) at 41; available at http://www.patientsafetyinstitute.ca/uploadedFiles/Resources/RCA_March06.pdf.

- *inadequate, defective, or obsolete tools, machinery, and equipment*
- *unusual circumstances (such as an emergency that requires workers to perform jobs they normally don't do)*
- *rarely performed jobs.*³⁰

[63] Root cause analysis is a component of a breach response plan or protocol which is formalized through adoption of a breach management policy.³¹ Such a policy provides direction by listing who requires notification upon learning of a breach, and what steps must be taken to adequately respond at that time.

[64] In Investigation Report F06-02, the benefits of having a breach protocol in place is explained as follows:

Breach Policy

[84] *Neither EFAP nor VCHA had policies—often referred to as a “breach protocol”—in place to direct organizational response to a privacy breach. Even with a policy, not all circumstances can be predicted or planned for. The process of determining an appropriate response is time-consuming, but becomes disproportionately so without the benefit of a policy to guide the response efforts. In addition, judgements on delicate issues in such an environment are often made under stress, which may produce a sub-optimal outcome. For these reasons, a policy prepared in advance can be indispensable.*

[85] *A breach policy should include a plan for dealing with the consequences of data losses. What is the scope of the data loss? What measures are required to contain the breach? If personal information is stolen, how might it be used? Who will be affected? Should affected individuals be notified and if so, how? What will be the content of notification and what risk-management strategies should you deploy to assist your clients in mitigating the risks to which they have been exposed? What information will you need to answer client questions in the event of a breach?*

[86] *A guide to responding to privacy breaches—which is not the same as an organization-specific breach policy, but that can be used to create one—is attached to this report as Appendix 5.*³²

³⁰ Saskatchewan Labour, Occupational Health and Safety, *Accident Investigations – A Guide for Committees and Representatives*, (October 2002) at 15; available at <http://www.labour.gov.sk.ca/safety/accidentinvestigations/AccidentInvestigationpart1.pdf>.

³¹ For instance, *What to do when faced with a Privacy Breach Guidelines for the Health Sector*, (Ontario Information and Privacy Commissioner); available at <http://www.ipc.on.ca/images/Resources/up-3hprivbreach.pdf>.

³² *Supra*, note 23

[65] After investigating a complaint, a report should be prepared including a description of what happened, an explanation of the cause(s), and what immediate or any long-term corrective action(s) will be taken. Responsibility for implementing corrective action must also be assigned. After implementation, the corrective actions should be monitored to ensure effectiveness. This type of plan, however, would only be engaged if potential privacy breaches become known to a person that has the requisite authority and resources to take action. It is also not possible to state with confidence that there were no other similar complaints. SK Health was unable to produce such a report.

[66] All privacy complaints should be documented and subsequently reported to the individual with delegated responsibility to investigate such complaints; most appropriately, this would be the Department's Privacy Officer. Without active monitoring of the system, including logging incidents, there is no way to gauge whether a system is operating smoothly or not. To our knowledge, neither department has such a monitoring system in place.

[67] From receipt of the first complaint, it was evident that SK Health did not have a formal process in place for routing complaints to one central contact. We noted as follows:

Our office has received a complaint from [the complainant] of [town], [province]. We will investigate pursuant to section 52 and section 42(1)(c) of The Health Information Protection Act.

[The complainant] reports that he received a letter from Saskatchewan Health, Drug Plan, Extended Benefits, on Monday, January 26, 2004. The letter was inside an envelope that was unsealed.

A photocopy of the letter, dated January 16, 2004, and the envelope is attached. On January 26, 2004, [the complainant] reports that he spoke to [the Director, System and Client Support Services] of Saskatchewan Health. [The Director, System and Client Support Services] apparently identified himself as the head of that department and the appropriate person to address the matter of the unsealed envelope. [The complainant] reports that the glue on the envelope is untouched and undisturbed.

... [The Director, System and Client Support Services] was given the post date on the envelope and then confirmed that the letter in question would have been sent directly from his department. [The Director, System and Client Support Services] undertook to investigate and then to advise [the complainant] of his findings.

*On March 18, 2004, when [the complainant] had not heard from [the Director, System and Client Support Services] he telephoned Saskatchewan Health for a report on the internal investigation. **At that time, he was advised that the person he should speak with was** [the Executive Director of SK Health]. Although messages were left for [the Executive Director], [the complainant] reports he received no call back.*

The complaint then is two-fold:

- 1. How did the letter come to be sent to [the complainant] in an unsealed envelope? What processes are in place to prevent a security breach?*
- 2. Why has Saskatchewan Health failed to report to [the complainant] on its investigation?*

I would ask that you look into this matter and then advise us as to the position of Saskatchewan Health.

[Emphasis added]

[68] Our main contact with SK Health with respect to privacy issues changed three times during the course of this investigation:

- Director, Strategic Planning and Information Policy, until August 28, 2005;
- Privacy Officer, Health Information Policy and Analysis, Director, October 1, 2005 to May 4, 2006; and
- the present Director Health Information Policy and Analysis and Chief Privacy and Access Officer, commenced May 23, 2006.

[69] In addition to these three individuals, our office also had contact with eight different individuals from each of the two departments.

[70] Our office has repeatedly addressed the importance of leadership within government institutions to ensure full statutory compliance³³. There is no substitute for a well-trained senior person with the responsibility for FOIP and HIPA compliance throughout their organization. Just as important is that any loss of continuity is minimized by careful planning to deal with the transition from one individual to another. I encourage SK Health to ensure that planning is implemented now so that the important work of the Privacy Officer is protected in any future personnel change. Action taken now can ensure that future Privacy Officers for SK Health can very quickly become familiar with all

³³ Office of the Saskatchewan Information and Privacy Commissioner, *Investigation Report H-2005-002; Investigation Report F-2007-001; Report F-2006-003; 2003-2004; Annual Report; 2004-2005 Annual Report; 2005-2006 Annual Report; 2006-2009 Business Plan; FOIP FOLIO*, (December, 2005 and September, 2006); all available at www.oipc.sk.ca

ongoing investigations and be better equipped to ensure no prejudice to complainants results from a changeover.

[71] When asked if its branches have a system in place to track complaints about unsealed envelopes, SK Health responded as follows:

The majority of Branches do not have a system to track complaints, as most Branches have not received complaints. Three Branches reported having a system to track complaints, which includes maintaining a record of complaints and relaying those complaints to SPM, initiating an investigation by SPM, and follow-up directly with the complainant to obtain the detail of the complaint. Complainants are informed of their right to contact the Department Privacy Officer or the Office of the Saskatchewan Information and Privacy Commissioner if their privacy concerns are not solved to their satisfaction.

[72] SK Health has made a significant improvement by implementing this type of complaint tracking system. However, there does not appear to be a mechanism or requirement for SPM to track and report complaints to SK Health's Privacy Officer about mail it processed on SK Health's behalf.

[73] Additionally, SK Health informed us of the following efforts and improvements made to address concerns with respect to mail handling procedures:

1. SK Health reviewed mail handling procedures with its staff. In its November 3, 2005 letter to us, SK Health explained that,

[b]oth the Drug Plan and Extended Benefits and Health Registration and Vital Statistics Branches have communicated to their staff the importance of ensuring envelopes are handled in a way as to minimize the potential for envelopes arriving at their destination unsealed.

This communication was done verbally and via email.

2. On April 21, 2005, the Department explained that some communication was done with SPM, but messaging did not reach everyone initially as demonstrated by the following:

The Director of Mail Services at Property Management (formerly SPMC) is [name of employee]. He took over from [the Director of Mail Services] who retired in December 2004. Further to a conversation with [the Director, Systems and Client Support Services] on April 18, 2005, [the Director of Mail Services] did do some checking into what communication

might have gone out from [the retired Director of Mail Services (as of December 31, 2004)] when contacted in 2004 about an envelope entering the mail unsealed. [The Director of Mail Services] learned that an e-mail was not circulated, and further to that personnel involved on the mail services front line do not have a computer and access to e-mail.

[The Director of Mail Services] did talk with the Operations Manager of Mail Services in Central Sort (office adjacent to the mail services area), and she did confirm that she was aware of the incident, so [the retired Director of Mail Services] had done some communications about the incident.

Further to the above, [the Director, System and Client Support Services] and [the Executive Secretary – direct supervisor of the Branch’s mail clerk and other staff involved in large mail outs] on April 19, 2005 made contacts with the sub-mailrooms at 3085 Albert Street and 3211 Albert Street to see if they were contacted by [the retired Director of Mail Services]. The operators for both of the sub-mailrooms do not recall being contacted regarding the incident.

3. SK Health informed us by way of letter dated November 3, 2005 that the following was shared in writing with its and SPM’s relevant personnel:

Recognizing there is always room for improvement in any process or procedure, our Department has brought this matter to the attention of SPM encouraging SPM to review its current processes and to work with its staff to try to avert the possibility of further envelopes being delivered unsealed.

The Department has also issued a memo to its Senior Administrative staff bringing this matter to their attention. The memo provides support staff with information about how envelope sealant may deteriorate when exposed to the sun or to heat vents. It also highlights that the use of glue stick may interfere with the envelope’s sealant possibly contributing to the delivery of an unsealed envelope. The memo recommends that branches consider environmental effects on storage of envelopes and to discontinue the use of glue sticks for sealing envelopes. The memo further recommends that branches consider sealing individual or small number bulk envelopes containing confidential information prior to them leaving the Department.

Both the Drug Plan and Extended Benefits and Health Registration and Vital Statistics Branches have communicated to their staff the importance of ensuring envelopes are handled in a way as to minimize the potential for envelopes arriving at their destination unsealed.

- a. The memo referenced above is reproduced below:

Through our discussions with Mail Services, we have learned that there are some Department practices that can contribute to envelopes

arriving unsealed at their destination. These include proper storage of envelopes before use and the use of glue sticks.

When envelopes are stored in locations where they are exposed to the sun or to heat vents, the sealant on these envelopes can become compromised and contribute to sealed envelopes becoming unsealed prior to arriving at their destinations. It is therefore important to ensure new envelopes are not exposed to these conditions.

Sealing envelopes with glue sticks is also problematic because the glue interferes with the envelope's sealant and may cause the envelope to become unsealed prior to arriving at its destination. For this reason, it is important that glue sticks are not used to seal envelopes.

Although not practical for large mail-outs, I would like to recommend for all individual and small bulk mail-outs containing personal health information, certificates or cards be sealed prior to leaving the Department. [Employee's name], Director of Mail services at Saskatchewan Property Management (SPM) has stated that SPM prefers envelopes containing confidential or sensitive information be sealed before his Department picks up this mail.

- b. The relevant portions of SK Health's letter to SPM, also dated November 3, 2005, are as follows:

As you know from previous discussions with staff from Saskatchewan Health, the Saskatchewan Information and Privacy Commissioner has two active reviews pertaining to the delivery of unsealed envelopes originating from our Department. During those conversations you provided information about how the Department's mail is picked up, processed and delivered to Canada Post by Saskatchewan Property Management, Mail Services.

From those discussions, our Department is satisfied that the Mail Services processes currently in place meet our needs and industry standards. However, given that there are a small number of envelopes reaching our intended recipients unsealed, we would ask that Mail Services consider reviewing its processes to decrease the potential for envelopes arriving at their destinations unsealed. We would also appreciate Mail Services working with staff to further ensure that all envelopes arrive at their destinations sealed.

[74] Now that I have determined what safeguards SK Health had in place and what improvements were made, I will consider recommendations from other Commissioners after undertaking investigations into similar complaints.

[75] In the case of an investigation by the Privacy Commissioner of Canada's office in which a complainant alleged that her bank sent her copies of applications for investments in two unsealed envelopes, the bank responded as follows:

The bank confirmed that it had mailed two transactions to the complainant but in one envelope, not two. It explained that mail leaving the branch was sealed and stamped at its offsite facility. Envelopes were fed through a sealing machine simultaneously and, according to the bank, it was possible but rare that an unsealed envelope could leave the system. The bank has a quality assurance process in place that involves inspecting a number of processed envelopes before they are mailed. The bank also stated that its machinery was working correctly at the time in question and that it had not received any other complaints of unsealed envelopes.

...

Application: *Principle 4.7 states that personal information must be protected by security safeguards appropriate to the sensitivity of the information. Principle 4.7.1 states that security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification and that organizations must protect personal information regardless of the format in which it is held.*

In a similar case involving a different bank, the envelope in question was made available to the Office of the Commissioner and therefore could be examined to verify the condition of the seal and glue. It was not possible in this case to verify the state of the seals, since the complainant did not keep the envelopes. Therefore, there was insufficient evidence for the Commissioner to conclude that the bank failed to properly safeguard the complainant's personal information as per its obligations under Principles 4.7 and 4.7.1.

He concluded that the complaint was not well-founded.

Further Considerations

Although there was insufficient proof to determine whether the envelope(s) were unsealed when they were sent to the complainant, the potential nevertheless existed. The Commissioner therefore recommended that the bank institute a policy that all mail be sealed prior to leaving the branch and being transported to the offsite mailing facility. In his view, if staff at the outside facility also continue to check the seals on outgoing envelopes, the safeguarding of client's personal information will be significantly improved.³⁴

[76] In PIPEDA Case Summary #154, the Privacy Commissioner of Canada investigated a complaint from a husband and wife who received from their bank mortgage documents in an unsealed envelope. The envelope in question did not appear to have ever been sealed.

³⁴ Privacy Commissioner of Canada, *PIPEDA Case Summary #197*, available at http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030801_02_e.asp.

Though the Commissioner accepted the explanation from the bank that the envelope went unsealed due to a rare mechanical error in a normally well-functioning piece of equipment, the following was also concluded:

Still, the fact remained that an error of some consequence had occurred. Though immediately attributable to mechanical, not human, malfunction, it was nonetheless an error that had gone undetected by human beings who were under an obligation to keep personal information secure. Furthermore, though no actual disclosure appeared to have occurred, it was an error that had created a significant potential for disclosure of exactly the sort the complainants had feared.

In sum, the Commissioner determined that, notwithstanding that its consequences had proved less serious than imagined, it was an inexcusable error that clearly reflected a lack of appropriate safeguards for protecting personal information against unauthorized access. He found therefore that the bank had been in contravention of Principles 4.7 and 4.71.

He concluded that the complaint was well-founded.

Further Considerations

Though pleased that the remedial measures taken at the branch in question, the Commissioner did not believe that these went far enough. He observed that, wherever there is reliance on machinery in the processing of sensitive personal information, there must also be reliance on a human element to ensure the security of the information thus processed. He recommended that the bank reinforce, not only at the branch in question but at all branches across Canada, appropriate procedures for verifying that envelopes to be mailed to customers are sealed.³⁵

[77] In an Order by the Information and Privacy Commissioner of Prince Edward Island, the Commissioner offered the following:

While I realize that it is virtually impossible to completely eliminate all human or technical errors which result in invasions of privacy, I expect to be able to assure the public that policies and procedures are in place to safeguard their personal information.

I find that, with the installation of new envelope stuffing equipment, the Public Body has taken steps to minimize improper disclosures of personal information such as this one from occurring in the future. The Public Body should also ensure that the technicians who use such equipment receive training regarding the requirements of the Act relating to protection of privacy. The Third Party and the public at large should find some comfort in this. In addition, the public and the

³⁵ Privacy Commissioner of Canada, *PIPEDA Case Summary #154*, available at http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030415_1_e.asp.

Act will be better served once the Public Body has set in place a procedure to investigate future events such as these.

...

*In order for the public to have confidence in laws such as the Freedom of Information and Protection of Privacy Act, Public Bodies must be seen to take extreme care carrying out their obligations under the Act. An individual whose privacy has been compromised must be advised not only why it was compromised, but how it will be prevented in the future.*³⁶

[78] On April 10, 2007, SK Health summarized its position as follows:

*Prior to reaching the conclusion indicated by [SK Health's Privacy Officer, Health Information Policy and Analysis, Director] in her November 2, 2005 letter to [SPM's Director of Mail Services], staff from Saskatchewan Health had several discussions with [the Director of Mail Services] regarding the mail services provided by Saskatchewan Property Management (S.P.M.). During these conversations, [the Director of Mail Services] provided information about how the Department's mail is picked up, processed and delivered to Canada Post by the S.P.M. Mail Services Branch. **From these discussions, Saskatchewan Health reached the conclusion that Saskatchewan Health is satisfied with the mail services processes provided by S.P.M.** [The Privacy Officer, Health Information Policy and Analysis, Director from October 1, 2005 – May 4, 2006] also requested, in a letter to [the Director of Mail Services], **that given that there are a small number of envelopes reaching our intended recipients unsealed, that the S.P.M. Mail Services Branch consider reviewing its processes to decrease the potential for envelopes arriving at their destinations unsealed.** In addition, [the Privacy Officer, Health Information Policy and Analysis, Director from October 1, 2005 – May 4, 2006] asked that the Mail Services Branch work with staff to further ensure that all envelopes arrive at their destinations sealed.*

[Emphasis added]

[79] SK Health also informed us that in the upcoming months its Policy and Planning Branch will be formalizing its internal mail handling processes through the development of a standard written policy. This does not, however, address the mail SPM seals on its behalf.

[80] A helpful Alberta Government publication provides some considerations for those organizations relying on others to provide services on its behalf:

Particular care should be taken in defining the contractor's responsibilities and obligations when the contractor will be handling personal information on behalf of the public body. These contracts require a greater level of detail than

³⁶ Prince Edward Island Information and Privacy Commissioner, *Order PP-04-003* at 8 and 9; available at <http://www.assembly.pe.ca/foipp/PP-04-003.pdf>.

*contracts that do not involve personal information, including specification of the type of physical protection to be used in the contractor's office (including a home office), the methods for transmitting data between the contractor and the public body and the limitations on use and disclosure of the information by the contractor.*³⁷

...

*Outsourcing has been used for the delivery of various services, including information technology services, safety and technical inspections, highway maintenance, registry services, government licensing functions, and the operation of programs and facilities. The public body remains accountable for the program and the performance of the service provider.*³⁸

*The Government of Alberta encourages ministries to consider the protection of personal information when contracting for services that involve the processing or storage of personal information. Apart from the high level of protection afforded by Alberta's privacy legislation, there is a relatively high level of understanding and legal certainty about the application of Alberta's privacy legislation. In particular, it is well established that under the FOIP Act a public body is responsible for the protection of personal information by a contractor acting on its behalf.*³⁹

[81] Also on this issue, I considered a helpful resource on the application of Ontario's health information protection law, *The Personal Health Information Protection Act – Implementing Best Privacy Practices*. Of relevance is the following section:

Health information custodians [equivalent to trustees in Saskatchewan] intending to hire third parties should investigate whether potential agents have themselves already taken steps to comply with applicable privacy laws. Through both interviews and investigation, custodians should determine whether potential agents have:

- *appointed a privacy officer,*
- *developed a written policy,*
- *assessed security risks, understood legal requirements, and taken steps to address any risks,*
- *adopted reasonable security standards,*
- *demonstrated a commitment to privacy, and*
- *effectively trained and sensitized staff to privacy – and security – related issues.*

³⁷ Government of Alberta, *Managing Contracts under the FOIP Act, A Guide for Government of Alberta Contract Managers and FOIP Coordinators, Discussion Draft*, (September 2005) at 11; available at <http://foip.gov.ab.ca/resources/publications/pdf/contractmanager.pdf>

³⁸ *Ibid*, at 12

³⁹ *Ibid*, at 36

*...Failing to ask agents to confirm the latter could leave the custodian paying a supplier who needs to shore up technology, security or information-handling or storage practices.*⁴⁰

- [82] As explained earlier, SK Health does not have a written agreement with SPM that would clarify its service expectations based on legislative requirements.
- [83] Due to the sensitivity of the personal information/personal health information involved and potential for harm, encouraging SPM to review its practices is insufficient; SK Health should instead enter into a formal written agreement with SPM to ensure its obligations under section 16 of HIPA are met.
- [84] Both departments provided some direction to employees in terms of what practices to avoid as they may contribute to envelopes arriving unsealed at their destination (i.e. do not store envelopes close to heat vents). This instruction and the utilization of the new mail sealing unit at Central Sort may mitigate future risks somewhat. However, I find that as the departments do not have in place: (a) a mechanism for two-way tracking and reporting of complaints,⁴¹ (b) appropriate procedures for investigating privacy complaints once received, and (c) a written agreement, SK Health has not met the standard of reasonableness in the circumstances.
- [85] In my Investigation Report F-2007-001, in terms of sending sensitive personal information/personal health information through the mail, I recommended the following:

[233] I start from the position that the personal information and personal health information in the possession of WCB is sensitive and prejudicial. It comprises in very large part either personal health information or personal financial information. It includes detailed diagnostic, treatment and care information from an array of primary providers and specialists. It includes particulars of compensation received from either WCB or through one's employment.

[234] I do not understand the provision in the procedures of WCB that requires someone to designate whether or not material in any given claim file is or

⁴⁰ Graham W.S. Scott et al., *The Personal Health Information Protection Act – Implementing Best Privacy Practices*, (Canada: Butterworth, 2005) at 93 & 94.

⁴¹ A resource that provides instructions for setting up a complaint-handling process is a publication from Government of Alberta, *Setting Up A Complaint-Handling Process*, (December 2004); available at <http://www.psp.gov.ab.ca/resources/pdf/ComplaintHandling.pdf>.

contains “sensitive information”. Given the business of WCB, I strongly encourage WCB to view all of its claims files and their contents as “sensitive information” and treat it accordingly.

[235] *I find that it is inappropriate to send out claim file material to any claimant by ordinary mail. Although I have no evidence that an improper disclosure resulted from WCB actions, in this case that risk remains. In the result, WCB failed to adequately safeguard this information.*

...

[237] *I further recommend that a double envelope system be adopted. The outside envelope would have the name of the claimant and address. The inside envelope should have a bold notice to the effect:*

THIS DOCUMENT IS CONFIDENTIAL AND IS TO BE OPENED ONLY BY THE ADDRESSEE.⁴²

[86] By adopting such a system when mailing out personal health information or other sensitive personal information, SK Health would be modeling a privacy best practice.

[87] We note the heightened awareness and significant improvements in SK Health’s internal processes. If the Department acts on the recommendations in this Report it will be adopting measures that will better enable it to meet its section 16 of HIPA obligations with respect to mail handling.

[88] I offer our thanks to both departments, especially SK Health’s Director Health Information and Policy and Analysis and Chief Privacy and Access Officer, for fully cooperating with our office throughout this investigation.

VI. RECOMMENDATIONS

[89] I recommend that SK Health ensure that SPM’s mail processing systems and procedures are audited to determine why some envelopes do not seal properly: once completed, ensure that necessary short and long term strategies identified through the process are implemented.

⁴² Available at: <http://www.oipc.sk.ca/Reports/InvReportF-2007-001.pdf>

- [90] I recommend that SK Health enter into a formal written agreement with SPM with respect to mail handling procedures and build into the agreement mechanisms to ensure privacy protection.
- [91] I recommend that SK Health in conjunction with SPM develop a formal complaints tracking system with direct reporting to SK Health's Privacy Officer.
- [92] I recommend that SK Health develop a breach response protocol to respond to reports of potential privacy breaches.
- [93] In the interim, I recommend that SK Health either seal or flag as sensitive all envelopes containing personal health information prior to its transport to SPM. If envelopes are only flagged, then SK Health must ensure that SPM adheres to strict security protocols and procedures such as double checking seals prior to the mail being picked up for delivery and employing the double envelope system.
- [94] Finally, I recommend that the Department provide the second complainant with a written apology forthwith.

Dated at Regina, in the Province of Saskatchewan, this 6th day of June, 2007.

R. GARY DICKSON, Q.C.
Saskatchewan Information and Privacy Commissioner