SASKATCHEWAN

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT H-2013-002

Regina Qu'Appelle Regional Health Authority

Summary: In May 2010, the media alerted the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) to seventeen addressograph cards found strewn about the ground near two facilities of a document destruction company in Regina, fifteen of which were later to be found belonging to the Regina Qu'Appelle Regional Health Authority (RQRHA). The addressograph cards were apparently found by a member of the public who contacted the Regina Police Service. The Commissioner undertook an investigation on an own motion basis after RQRHA informed his office of details of the breach. Even though the displacement of the addressograph cards was the result of actions by an employee of the document destruction company, the Commissioner found that RQRHA was responsible for the actions of its Information Management Service Provider. The Commissioner found that RQRHA had inadequate safeguards in place to ensure the proper destruction of the addressograph cards in question. Therefore, he recommended that RQRHA supplement and formalize its written procedure in regards to the disposal of records containing personal health information and that RQRHA conduct regular and ongoing audits of the document destruction company to help prevent a similar future occurrence.

Statutes Cited: *The Health Information Protection Act* S.S. 1999, c. H-0.021, ss. 2(j), 2(m), 2(t)(ii), 16, 17(2)(b), 18(1), 42(1)(c), 52.

Authorities Cited: Saskatchewan OIPC Review Reports F-2008-002, LA-2009-002/H-2009-001; SK OIPC Investigation Reports H-2010-001, H-2011-001, H-2013-001.

Other Sources Cited: Saskatchewan OIPC, *Letter to the Speaker on Bill 61, The Vital Statistics Act 2007* (May 9, 2007); SK OIPC *Glossary of Common Terms: The Health Information Protection Act (HIPA)*; *Regina Qu'Appelle Health Region 2009-2010 Annual Report*, *Regina Qu'Appelle Health Region Incident Review Report Addressograph Cards Breach*, July 23, 2010; Royal Canadian Mounted Police, *Identity Theft and Identity Fraud*; National Association for Information Destruction, Inc. *Information Destruction Policy Compliance Toolkit*. Version 1, April 2008; Regina Qu'Appelle Regional Health Authority, *Personal Health Information Protection*, Policy Reference Number: 501, Effective Date: October 20, 2005, *Personal Health Information Protection*, Procedure Reference Number 501-1, Effective Date: October 20, 2005.

I BACKGROUND

[1] The Office of the Saskatchewan Information and Privacy Commissioner (OIPC) was alerted by the media on May 20, 2010 that seventeen addressograph cards were found strewn about the ground near two facilities belonging to a document destruction company in Regina by a member of the public. This individual contacted the Regina Police Service (RPS).

[2] My office received a letter dated May 21, 2010 from the Regina Qu'Appelle Regional Health Authority (RQRHA)[1] notifying us of the breach. RQRHA provided me with general details of the incident, advised that it would undertake a privacy review and that it would share its findings with this office.

[3] The document destruction company is the contractor RQRHA used to destroy its addressograph cards.

[1] "*The Regional Health Services Act* establishes the Regina Qu'Appelle Regional Health Authority (hereinafter RQRHA) as the governing body of the Regina Qu'Appelle Health Region (hereinafter RQHR)." *Regina Qu'Appelle Health Region 2009-2010 Annual Report* at p. 9, available at www.health.gov.sk.ca/regina-quappelle-annual-report-2009-10.

[4] Fifteen of the seventeen addressograph cards contained personal health information and were from the Regina General Hospital and the Pasqua Hospital.[2] The other two addressograph cards were found to belong to another trustee. My office undertook a separate investigation of that incident.

[5] RPS apparently took witness statements from both the member of the public who found the cards and the CEO and President of the document destruction company. RPS also seized the addressograph cards in question.

[6] On or about July 15, 2010, my office sent a letter to RQRHA notifying it that my office was undertaking an investigation on an own motion basis pursuant to sections 42(1)(c) and 52 of *The Health Information Protection Act* (HIPA).[3]

[7] I spoke with legal counsel of RPS on July 21, 2010. It was determined that my office would be the appropriate agency to deal with this particular matter given the explicit mandate under section 52 of HIPA. Therefore, RPS provided my office with the addressograph cards in question, copies of the witness statements, and RPS *Occurrence Report*.

[8] Further, as a result of my discussions with RPS, we agreed that at the conclusion of my office's investigation, we would make arrangements so that the addressograph cards would be properly destroyed.

[9] On July 23, 2010, RQRHA sent my office its *Incident Review Report*[4] – a result of its privacy review. The *Incident Review Report* included:

- details of when and how the addressograph cards were discovered,
- the types of personal health information that is contained on addressograph cards,

[2]Both the Regina General Hospital and the Pasqua Hospital are a part of the Regina Qu'Appelle Regional Health Authority.
[3]*The Health Information Protection Act*, S.S. 1999, c. H-0.021 (hereinafter HIPA).
[4]*Regina Qu'Appelle Health Region Incident Review Report Addressograph Cards Breach*, July 23, 2010.

- how RQRHA notified affected individuals through registered mail, and
- its conclusions and recommendations of how to prevent similar occurrences.[5]

[10] My office requested and received more information pertaining to the incident and information regarding relevant documents such as a copy of the contract between RQRHA and the document destruction company and RQRHA's written procedure for handling addressograph cards destined for destruction from RQRHA.

[11] Once my office's investigation was complete, we provided a preliminary analysis that included recommendations on August 10, 2012.

[12] RQRHA did not comply with all of my office's recommendations. Therefore, my office notified RQRHA on October 24, 2012 that I would issue a public Investigation Report.

II ISSUES

1. Was the information contained on the addressograph cards "personal health information" as defined by section 2(m) of *The Health Information Protection Act*?

2. Is Regina Qu'Appelle Regional Health Authority in compliance with section 18(1) of *The Health Information Protection Act*?

3. Did Regina Qu'Appelle Regional Health Authority have sufficient safeguards in place to reasonably protect against a similar incident from occurring again?

III DISCUSSION OF THE ISSUES

1. Was the information contained on the addressograph cards "personal health information" as defined by section 2(m) of *The Health Information Protection Act*?

[5] *Ibid.*

[13] Section 2(t)(ii) of HIPA states as follows:

> **2** In this Act:
>
> ...
>
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> ...
>
> (ii) a regional health authority or a health care organization;[6]

[14] Therefore, RQRHA, as a regional health authority, is a "trustee" for the purposes of HIPA.[7]

[15] Section 2(m) of HIPA defines "personal health information" as follows:

> **2** In this Act:
>
> …
>
> (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;[8]

[6] *Supra* note 3.
[7] I previously found that RQRHA is a trustee for the purposes of HIPA at [28] of my Investigation Report H-2013-001, available at www.oipc.sk.ca/What's%20New/IR-H-2013-001/Investigation%20Report%20H-2013-001.pdf and at [27] of my Review Report LA-2009-002/H-2009-001, available at www.oipc.sk.ca/Reports/LA-2009-002%20and%20H-2009-001,%20December%2017,%202009.pdf.
[8] *Supra* note 3.

[16] RQRHA's *Incident Review Report* dated July 23, 2010 stated that the addressograph cards contained the following information:

> An addressograph card contains the following information, though it may not be understood by individuals outside of the RQHR:
>
> - name
> - abbreviation for the facility visited
> - date of birth
> - gender
> - medical record number (MRN). This is a number used internally by the RQHR to manage files and cannot be used for other purposes outside of the RQHR
> - Hospital Services Number (HSN)
> - name of the admitting physician
> - name of the family physician
> - date of visit
> - address
> - visit number. This is a number used internally by the RQHR and cannot be used for other purposes outside of the RQHR[9]

[17] Based on the list of the data elements contained on an addressograph card provided to my office by RQRHA and the definition of "personal health information" found in section 2(m) of HIPA, it is clear that the addressograph cards contain personal health information.

[18] In my letter dated May 9, 2007 to the Speaker of the Legislative Assembly concerning Bill 61, *The Vital Statistics Act, 2007*, I stated that according to the Royal Canadian Mounted Police (RCMP), two of the three "key pieces of information" sought by identity thieves suspects are a person's name and date of birth.[10] Further, the RCMP has noted that the following are the pieces of information identity thieves seek:

> Identity thieves are looking for the following information:
>
> - **full name**
> - **date of birth**
> - Social Insurance Numbers
> - **full address**

[9] *Supra* note 4.
[10] Office of the Saskatchewan Information and Privacy Commissioner (hereinafter SK OIPC), *Letter to the Speaker on Bill 61, The Vital Statistics Act 2007*, (May 9, 2007); available at www.oipc.sk.ca/webdocs/vitalstats.pdf.

- mother's maiden name
- username and password for online services
- driver's license number
- personal identification numbers (PIN)
- credit card information (numbers, expiry dates and the last three digits printed on the signature panel)
- bank account numbers
- signature
- passport number[11]

[emphasis added]

[19] Given that the name, date of birth and address along with a whole host of other personally identifying information appears on addressograph cards, the loss of such information may prove to have serious consequences for individuals.

2. Is Regina Qu'Appelle Regional Health Authority in compliance with section 18(1) of *The Health Information Protection Act*?

[20] Section 2(j) of HIPA defines "information management service provider" (IMSP) as follows:

> **2** In this Act:
> …
>
> (j) **"information management service provider"** means 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;[12]

[21] Since the document destruction company destroys addressograph cards on behalf of RQRHA, it is an IMSP.

[22] Section 18(1) of HIPA states as follows:

[11]The Royal Canadian Mounted Police (RCMP) *Identity Theft and Identity Fraud*. www.rcmp-grc.gc.ca/scams-fraudes/id-theft-vol-eng.htm, accessed June 15, 2012.
[12]*Supra* note 3.

> **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;
>
> (b) to enable the information management service provider to provide the trustee with information management or information technology services;
>
> (c) for the purpose of having the information management service provider take custody and control of the personal health information pursuant to section 22 when the trustee ceases to be a trustee; or
>
> (d) for the purpose of combining records containing personal health information.[13]

[23] In my Investigation Report H-2011-001, I considered in detail the elements that any trustee should consider when contracting with an IMSP generally and those elements relevant specifically to the storage, transportation or destruction of personal health information.[14]

[24] To determine the adequacy of the contract between RQRHA and the document destruction company, I requested a copy of the contract in my office's letter dated August 10, 2011. RQRHA provided a copy of the contract enclosed with its letter dated November 3, 2011 to my office. The contract is in effect for the time period October 1, 2010 to September 30, 2013.

[25] The portions of the contract that are relevant to this matter are as follows:

> …
>
> 7. Employees of the Contractor Bound
>
> The Contractor and Region hereby further acknowledge and agree that, in order for the Contractor to fulfil [sic] its service obligations under the Agreement, the Contractor shall be permitted to grant its employees access to PI. The contractor hereby agrees that:

[13] *Ibid.*
[14] SK OIPC Investigation Report H-2011-001 at [197] to [203], available at www.oipc.sk.ca/Reports/IR%20H-2011-001.pdf.

(a) it will make only make PI available to its employees to the minimum extent necessary for the purpose of fulfilling the Contractor's obligations under the Agreement; and

(b) **it will cause, or has caused, each of its employees providing services on behalf of the Contractor under the Agreement to agree, in writing, to protect the confidentiality and security of the PI to at least the extent provided by this Schedule.**

The Contractor will properly advise and train each of its employees providing services under the Agreement of the requirements of the Contractor under this Schedule and HIPA and LAFOIPPA. The Contractor specifically assumes all responsibility for its employees for the breach by any of them of any provisions of this Schedule or such laws.

8. Audit

The Contractor will provide (a) Region's internal auditor; and/or (b) a nationally recognized Canadian audit firm appointed by Region, upon fifteen (15) days prior written notice, with reasonable access to relevant books, records and facilities related to the Agreement in order to conduct appropriate audits, examinations and inspections to ensure the Contractor's compliance with this Schedule.

Except as otherwise provided below, such audits, examinations and inspections will be conducted at Region's expense and may be conducted periodically during the term of the Agreement, but not more than once per year.

The Contract will provide access to information and facilities reasonably required by Region's auditors to perform such audits.

…

12. Security and Segregation of PI

The Contractor shall have in place reasonable policies, procedures and safeguards to protect the confidentiality and security of the PI. The Contractor shall ensure the physical security of the PI by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. Such security arrangements shall include, without limitation, reasonable technical, physical and administrative safeguards. Without limiting the generality of the foregoing, the Contractor shall take reasonable steps to ensure that all PI is securely segregated from any information owned by the Contractor or third parties, including access barriers, physical segregation and password authorization.

…

14. Assistance with Complaints/Investigations

The Contractor shall co-operate with, and assist in, any investigation of a complaint that any PI has been collected, used or disclosed contrary to HIPA, LAFOIPPA or other applicable laws, whether such investigation is conducted by Region itself or a body having the legal authority to conduct the investigation. For greater certainty, the foregoing shall apply in respect of any formal or informal review or investigation conducted by the Office of the Information and Privacy Commissioner of Saskatchewan.

15. Privacy Representative

Immediately upon execution of this Agreement, the Contractor will appoint a representative to be responsible for the Contractor's compliance with this Schedule (the "Privacy Representative"). The Contractor will promptly provide Region with the name of its Privacy Representative and notify Region in a timely manner of any change of its Privacy Representative.

[emphasis added]

[26] As a trustee, RQRHA is responsible for the proper management of personal health information in its custody or control.[15] Even if the addressograph cards were in the custody of the document destruction company, RQRHA is still responsible for the proper destruction of the addressograph cards. Therefore, it is important to consider what type of training is provided to the document destruction company employees as it relates to managing personal health information. In assessing that material, I also considered industry standard and practices reflected in the National Association for Information Destruction, Inc.'s (NAID) *Information Destruction Policy Compliance Toolkit*.[16]

[27] Pursuant to paragraph 7 of the contract between RQRHA and the document destruction company, I need to know what type of training the document destruction company

[15]SK OIPC *Glossary of Common Terms: The Health Information Protection Act (HIPA)* defines **control** as "a term used to indicate records that are not in the physical custody of the trustee but are still within the influence of that body via another mechanism (i.e. contracted service, trustee employees working remotely, etc.). See Report F-2008-002 (Ministry of Justice and Attorney General). The control question normally only arises if there is no 'custody' of the phi in question." It defines the term **custody** as "the physical possession of a record by a trustee." The glossary is available at www.oipc.sk.ca/Resources/HIPA%20Glossary%20-%20Blue%20Box.pdf.

[16]National Association for Information Destruction, Inc. (NAID) *Information Destruction Policy Compliance Toolkit*, Version 1, April 2008.

provides to its employees as it relates to managing personal health information. Page 18 of the document destruction company's policy and procedure manual states as follows:

> **Policy and Procedure for Employees**
>
> 1. Accept confidential material from the customer that is properly security in boxes, containers or bags.
>
> 2. Ensure the storage compartment of the truck is securely locked at all times.
>
> 3. Always remain with the vehicle in the event of an accident or mechanical failure.
>
> 4. Use cell phone to call your supervisor for help if needed. If in a serious accident notify the police.
>
> 5. Ensure the material is stored in the secure area of the plant and properly identified.
>
> 6. [The document destruction company] requires each employee to sign a "NO READ DECLARATION" as a condition of employment.

[28] As a part of its training, required by the contract between RQRHA and the document destruction company, the document destruction company has its employees sign a "Letter of Agreement" (found on page 19 of the document destruction company's policy and procedure manual). The agreement states the following:

> I agree to abide by the following terms and conditions at all times:
>
> - Place all confidential materials in the locked and/or white bags supplied by [the document destruction company]. Ensure an empty container is available to replace full containers when doing pick-ups.
> - **Keeps cargo compartments on trucks locked at all times when transporting confidential documents.**
> - Store containers filled with confidential materials in the locked compound in the plant until shredding is complete.
> - Never read any confidential material.
>
> [emphasis added]

[29] Page 17 of the document destruction company's policy and procedure manual states that:

> Employees are expected to sign the… confidentiality agreement, a copy of which will be placed in the personnel file. Any breach of the confidentiality policy will result in automatic termination of employment.

[30] This contract, although it came into effect after this particular privacy breach occurred, appears to address the issue of transporting addressograph cards. The contract, the policy and procedures and the "Letter of Agreement" that is required to be signed by employees, appear to be reasonable safeguards. Therefore, RQRHA is in compliance with section 18(1) in that it has a contract in place that outlines the roles and responsibilities of the IMSP.

[31] However, one thing that was troubling was the typed notes of the Director of Risk Management and Privacy Officer at RQRHA. He advised he went on a site visit to the document destruction company's facilities on June 4, 2010, soon after the addressograph cards were discovered. His typed notes from the site visit states as follows: "Not all staff are trained regarding confidentiality. Many are ESL."

[32] In a letter dated March 21, 2012 to RQRHA, my office asked the following question: "Are the staff who are not 'ESL' trained in their confidentiality responsibilities differently [sic] than those [who] are 'ESL'?"

[33] RQRHA clarified that "ESL" stands for English as a Second Language in its letter dated May 11, 2012 to my office. RQRHA enclosed a copy of the written notes by the Director of Risk Management and Privacy Officer, from the same site tour, which varies from the typed notes quoted above. The written notes stated as follows: "some not trained – most are, those managing confidential info [sic] are."

[34] I recommended that RQRHA conduct audits to ensure that any employee of the document destruction company who is undertaking the destruction of addressograph cards – and any other documents that contain personal information and/or personal health information – has "agree[d], in writing, to protect the confidentiality and security of the [personal information] to at least the extent provided by this Schedule", in accordance with the contract between RQRHA and the document destruction company.

[35] In its September 19, 2012 letter to my office, RQRHA stated it "met with representatives from [the document destruction company] and have been assured that this practice is in place."

[36] However, my recommendation was for RQRHA to conduct regular and ongoing audits. Page 60 of NAID's *Information Destruction Policy Compliance Toolkit* describes a protocol for auditing service provider compliance. The protocol includes requiring the submission of relevant operating documents by the service provider, an annual scheduled audit, and periodic unannounced audits. NAID states that when violations are discovered, they should be documented and remedial or disciplinary action should be determined.[17]

[37] RQRHA clarified in its October 10, 2012 response to my office that it "will **not** be conducting audits at [the document destruction company] on a regular and ongoing basis". [emphasis added] The contract between RQRHA and the document destruction company explicitly allows for audits. It is difficult to understand why RQRHA refuses to conduct regular and ongoing audits to ensure the proper destruction of addressograph cards. There is little comfort to be had if the contracts provides for proper safeguards such as audits but are not put into practice. How can RQRHA be sure that the document destruction company is fulfilling its duties listed in the contract without audits? In my view, it cannot be sure.

[38] Such a response is disappointing given the ongoing responsibility of RQRHA prescribed by section 16, 17(2)(b) and 18(1) of HIPA.

3. Did Regina Qu'Appelle Regional Health Authority have sufficient safeguards in place to reasonably protect against a similar incident from occurring again?

[17] *Ibid.* at p. 60.

[39] Section 16 of HIPA imposes a duty upon trustees, such as RQRHA, to adequately protect the personal health information it has in its custody or control. Section 16 of HIPA states as follows:

> **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 or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[40] A letter dated May 21, 2010 from RQRHA to my office stated that RQRHA uses a contractor, the document destruction company, to dispose of confidential material including addressograph cards. The document destruction company has two facilities located in Regina. In this particular case, it was reported that one of the document destruction company employees was transferring the addressograph cards (which were in a container with a lid) between the two facilities. Apparently, the lid was not secured onto the container. As a result, addressograph cards blew out of the top of the container during the transfer. The addressograph cards were discovered two days later by a member of the public.

[41] Although it appears the privacy breach was a result of actions of an employee of the document destruction company, RQRHA has the responsibility to ensure the personal health information it has in its control is adequately protected pursuant to section 16 and properly destroyed, in accordance with section 17(2)(b) of HIPA, which states as follows:

> **17**(2) A trustee must ensure that:
> ...

> (b) personal health information is destroyed in a manner that protects the privacy of the subject individual.[18]

[42] I have stated in my Review Report F-2008-002 that a contract is an indication of control.[19] As described earlier, RQRHA has a contract with the document destruction company to dispose of its addressograph cards. In this particular case, I find that while the addressograph cards were not in the custody of RQRHA, it had control of the addressograph cards through a contract.

[43] Therefore, in the following subsections of this Report, I will discuss what safeguards RQRHA had in place and if they are reasonably sufficient to prevent a similar incident from occurring again in the future.

[44] Before I proceed, I note that a contract with an IMSP is an example of an administrative safeguard. Since I have already discussed the contract between RQRHA and the document destruction company, I will now discuss other safeguards that RQRHA had in place.

a. Policies and Procedures

[45] In previous Review Reports and Investigation Reports, I have stated that section 16 of HIPA requires that a trustee establish written policies and procedures. For example, in Investigation Report H-2011-001, I stated the following:

> [91] HIPA prescribes that the trustee must establish policies and procedures to maintain administrative, technical and physical safeguards. These safeguards must protect the integrity, accuracy and confidentiality of the information. They must also protect against any reasonably anticipated threat or hazard to the security or integrity of the information; and the loss of, unauthorized access to, use or disclosure of the information.[20]

[18] *Supra* note 3.
[19] SK OIPC Review Report F-2008-002 at [27] to [30] available at www.oipc.sk.ca/Reports/F-2008-002.pdf.
[20] *Supra* note 14.

[46] Also, in my Investigation Report H-2010-001, I highlighted the importance of written policies and procedures:

> [40] Section 16 is one of the most important features of HIPA. Without comprehensive written policies and procedures, the risk that a trustee will fall short of its many statutory responsibilities is dramatically increased. We have attempted to underscore this feature in a number of our publications including Review Report H-2008-002 and Investigation Reports H-2007-001, H-2005-002 and H-2004-001.[21]

[47] My view is that this section is particularly important. It functions as the spine to the HIPA skeleton as it is linked to every other provision in HIPA.

[48] My office sent a letter dated August 10, 2011 to RQRHA asking for a copy of RQRHA's written procedure for handling addressograph cards destined for destruction. In its letter dated November 3, 2011, RQRHA stated that "[t]here is no formal policy on this subject. In progress."

[49] In our letter dated March 21, 2012, my office clarified that what we sought was the relevant written procedure, not policy. It responded in a letter dated May 11, 2012 as follows:

> Currently the RQHR does not have any written procedure to cover how to handle addressograph cards destined for destruction. Nursing units do however **instruct Unit Clerks on the proper handling of addressograph cards in the instructions provided to them.**
>
> [emphasis added]

[50] The instructions for Unit Clerks noted above were enclosed with its letter dated May 11, 2012 to my office. The instructions provide ten steps to be taken by a Unit Clerk when the nurse discharges the patient. Step eight states as follows (addressograph cards are referred to as "blue cards"):

> …
>
> 8. Put blue card in drawer. When recycle card box full send to admitting.

[21] SK OIPC Investigation Report H-2010-001 at [40], available at www.oipc.sk.ca/Reports/H-2010-001,%20March%2023%202010.pdf

[51] Step eight is quite vague. It leaves us with many questions such as:

- Which drawer is the Unit Clerk to place the addressograph cards in?
- Does the recycling card box only contain spent addressograph cards?
- Or does it contain other material?
- How are Unit clerks to know addressograph cards are to be separate from other material?
- Are the contents of the recycle card box easily accessible?
- Is it locked down?

[52] In my office's preliminary analysis, we advised that step eight should be revised so that Unit Clerks are clear that the spent addressograph cards should be kept secure and separate from any other material or documents.

[53] RQRHA's *Incident Review Report* stated that before the breach, addressograph cards would be delivered to one of the facilities of the document destruction company. Then the addressograph cards would be transported to a second facility by an employee of the document destruction company (about one city block away) to be shredded. This method was being used when the breach occurred. After the breach, the document destruction company changed its processes so that addressograph cards would be delivered directly to the second facility to be shredded.

[54] To confirm such a change in process, the President and CEO of the document destruction company sent an email dated July 20, 2010 to the Director, Risk Management & Privacy Officer of RQRHA that states the following:

> Since the incident regarding the health cards at our facility at [address of first facility]. [sic] [The document destruction company] trucks now off load the cards right at the grinder (which is located at [address of second facility]). The grinder operators know to destroy those cards immediately whenever they are delivered. I have personally monitored the system since the changes were implemented and I'm confident that it works well.

[55] Loading the addressograph cards directly to the second facility and avoiding the need to transfer the cards between the facilities would minimize the chances of losing addressograph cards between facilities. However, in the *Incident Review Report*, RQRHA stated the following:

> [The document destruction company] pointed out during the tour that a problem exists with health regions sending paper material for shredding that also contains plastic addressograph cards. When these cards are found in paper recycling, the cards must be manually removed from the conveyor belts, stored temporarily and then sent to the second facility which is equipped for shredding plastic. That storage and transportation exposes the cards to increased risk. **In response to this, RQHR will inform all facilities and employees of the importance of keeping plastic and paper materials separate and appropriately labeled.**[22]
>
> [emphasis added]

[56] In its letter dated May 11, 2012, RQRHA provided the following in regards to policies and procedures:

> A policy and procedure is currently under development on this topic. In the absence of a current policy and procedure, the Privacy Office has circulated a Privacy Alert on the proper handling of spent addressograph cards.

[57] It enclosed a copy of the *Privacy Alert*. The *Privacy Alert* is undated. It is signed off by RQRHA's Privacy Officer and was sent to the "Management Forum". The *Privacy Alert* provided as follows:

> A recent situation within the RQHR highlighted the need to ensure that all staff understand the proper process for addressograph cards meant for destruction.
>
> - When an addressograph card is no longer required for a patient admission to an RQHR facility, the card must be forwarded to the Registration department.
>
> - The Registration staff will dispose of the addressograph cards in a locked [the document destruction company] bin. **These cards will be placed in a bin separate from paper shredding.** These cards are destroyed using a separate process at [the document destruction company].
>
> As trustees of personal health information, it is our responsibility to be aware of our roles and responsibilities regarding the protection of clients' personal health

[22] *Supra* note 4.

> information under the [sic] *Health information Protection Act* and **the related RQHR polices [sic] and procedures.**
>
> [emphasis added]

[58] The *Privacy Alert* details the procedures for storing and safely destroying spent addressograph cards but is incomplete. For example, it does not include information as to how the cards will be forwarded to the Registration department securely and how often.

[59] Although RQRHA had stated that it had no formalized written policy or procedure in place to address the management of spent addressograph cards, at the bottom of the *Privacy Alert*, it lists RQRHA policy *Personal Health Information Protection*[23] as an applicable policy.

[60] The policy itself is very vague. There are four parts to the policy. The first part of the policy states as follows:

> As a trustee of personal health information, all RQHR staff shall maintain administrative, technical and physical safeguards that protect the integrity, accuracy and confidentiality of the personal health information, regardless of the storage medium.[24]

[61] The second part of the policy states that it had been created as a result of HIPA. The third part of the policy states that all RQRHA staff and agents are affected by the policy. The fourth part of the policy appears to be a reproduction of section 2(t) of HIPA, which is the definition of the term "trustee."

[62] It appears that the related procedure to the policy entitled *Personal Health Information Protection*[25] lists RQRHA's expectations, not procedures, in regards to the security of personal health information in all RQRHA departments. The relevant parts of this document reads as follows:

---

[23]RQRHA, *Personal Health Information Protection*, Policy Reference Number: 501. Effective Date: October 20, 2005.
[24]*Ibid.*
[25]RQRHA, *Personal Health Information Protection*, Procedure Reference Number: 501-1. Effective Date: October 20, 2005.

The RQHR department or program security procedures shall address the following areas:

1.1 Organization/Culture Procedures in the following areas will contribute to a privacy/security conscious organizational culture by outlining:

…

- confidentiality agreements

…

1.2 Internal Security The internal security procedures shall address the following areas:

…

- proper destruction of Personal Health Information

…

1.5 Educational Awareness The educational awareness procedures shall address the following areas:

- comprehensive and universal education to all department or program staff
- initial orientation and periodic reviews
- access to appropriate content – such as the Intranet Privacy Web Site for legislation, the Office of the Saskatchewan Privacy Commissioner, and the Intranet Policy Web Site for policies

1.6 Physical and Environmental Security The physical and environmental security procedure shall address the following areas:

…

- appropriate destruction of disposed records containing Personal Health Information

…

…

1.10 Data Management Security The data management security procedure shall address the following areas:

...

- Appropriate methods for destruction of disposed records containing personal health information

…[26]

[26] *Ibid.*

[63] Since both the policy and procedure described above are inadequate to manage addressograph cards, I recommend that the contents of the *Privacy Alert* be supplemented and then formalized into a written procedure to be followed by all RQRHA staff and agents. For example, it should describe what is the "proper" destruction of personal health information.

b. Education

[64] In my Investigation Report H-2011-001, I said it is unlikely a trustee would be in compliance with the HIPA requirements in question without fulfilling the following six requirements:

> (a) A specifically tasked privacy officer with a clear mandate and appropriate training;
>
> (b) **Extensive training of staff in HIPA requirements and provisions;**
>
> (c) **Comprehensive, clear and practical written policies and procedures that are reinforced through leadership and training of staff;**
>
> (d) Written contracts with IMSP's that specifically address the requirements of section 17 and 18 of HIPA;
>
> (e) Audit of use and disclosures of the [personal health information]; and
>
> (f) Effective enforcement action to follow any breach.[27]
>
> [emphasis added]

[65] Further in the same Investigation Report, I stated the following:

> [149] Our office has consistently stressed, for the last seven years, the importance of providing all staff of trustee organizations with practical, accessible, concrete and granular information about what they must do to comply with HIPA in the course of collection, use, disclosure of [personal health information], as well as access to and correction of that [personal health information].[28]

[27] *Supra* note 14 at [92].
[28] *Ibid.* at [149].

[66] In regards to training, RQRHA provided the following information in its letter dated May 11, 2012:

> The RQHR provides department specific training to all employees. Memos that are circulated are meant to be reminders of the training previously provided to the employees. Therefore the RQHR does not have a process that confirms that all RQHR employees have received, read and understood all memos.
>
> In absence of a current RQHR Policy or Procedure to address the destruction of spent addressograph cards, a Privacy Alert has been circulated to information all staff of the proper process.

[67] Without formal written policies or procedures, it is unclear as to what the training would be based upon. Policy 501 and its related procedure provide very vague guidance as to how to manage spent addressograph cards. The *Privacy Alert*, though, appears to provide some practical, concrete and granular information as to how staff should manage spent addressograph cards. The contents of the *Privacy Alert* should be supplemented and formalized into written procedure and made accessible to all staff. Procedures provide constant direction to staff, whereas a *Privacy Alert* is a one-time reminder.

[68] In response to my recommendations for the development of procedures pertaining to the destruction of addressograph cards, RQRHA responded in its September 19, 2012 and October 10, 2012 correspondence to my office, by saying it would develop a draft of a procedure that would be ready for internal review by the end of the current fiscal year. That delay is unreasonable.

V FINDINGS

[69] I find that the information on the addressograph cards is "personal health information" as defined by section 2(m) of *The Health Information Protection Act*.

[70] I find that the Regina Qu'Appelle Regional Health Authority does not have sufficient safeguards in place to reasonably protect against a similar incident from occurring again.

[71] I find that the Regina Qu'Appelle Regional Health Authority is only partially in compliance with sections 16, 17(2)(b), and 18(1) of *The Health Information Protection Act*.

VI RECOMMENDATIONS

[72] I recommend that Regina Qu'Appelle Regional Health Authority supplement and formalize the written procedure in regards to the disposal of addressograph cards containing personal health information immediately.

[73] I recommend that Regina Qu'Appelle Regional Health Authority conduct regular and ongoing audits with the document destruction company to ensure that any employee that is managing the destruction of any material from Regina Qu'Appelle Regional Health Authority has been sufficiently trained to manage material in accordance with *The Health Information Protection* Act requirements and each has signed the "Letter of Agreement."

[74] I recommend that within 30 days of receiving the addressograph cards from my office, Regina Qu'Appelle Regional Health Authority confirm to my office the secure destruction of the fifteen addressograph cards in question.

Dated at Regina, in the Province of Saskatchewan, this 26th day of February, 2013.

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