NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER
Review Report 19-204
Citation: 2019 NTIPC 21

File: 18-158-4
December 3, 2019

Background

On July 23, 2018, the Manager of Quality and Risk Management of the Hay River Health and Social Services Authority (HRHSSA) notified the Information and Privacy Commissioner of a breach of privacy, specifically, that a minor's social services chart had gone missing from the Social Services Department in February, 2018. HRHSSA notified the child's foster parents of the breach on June 14, 2018. The HRHSSA provided me with a *Breach of Confidentiality Report* dated June 19, 2018. On it, the information lost was described as:

> Screening reports, investigation reports, child family services status reports, child family services case notes, court orders, medical reports, parents information, family social history, foster parent information, birth certificate custom adoption information, child protection worker information, legal counsel information and incident reports.

On August 29, 2018 I wrote to the Manager of Quality and Risk Management and asked for additional information by September 30, 2018. On October 26, 2018, having received no response, I again wrote to the Manager and asked for a response by November 15, 2018. On November 19, 2018 I received an email from the Manager noting that she had just received the final report back from the external investigator and that she would respond once she had reviewed it. I received a further letter from the Manager on December 7, 2018 that set out the following:

a) The secretary went to file a document and the file could not be located.

b) Neither the internal or external investigation could identify how the file came to be missing.

c) The file has been reconstructed.

d) The foster parents were notified of everything that went missing, DHSS was notified according to the privacy breach policy and the IPC was notified according to the privacy breach policy.

e) Paper files are kept in a file room that is opened at 8:30 each morning and re-locked at 16:30 each week day. There is a file sign-in and sign-out process. Files identified as sensitive are locked in the Supervisor's office in the blue file cabinet.

f) The Social Services staff carried out a thorough search prior to reporting, as the belief was that file had been misfiled and would turn up. Staffing resources available were tasked to carry out the investigation and the availability of witnesses to be interviewed.

g) There had been no further developments in locating the file.

For the reasons set out below, I decided that a review was warranted in the circumstances pursuant to section 49.2 of the *Access to Information and Protection of Privacy Act* (ATIPPA).

Relevant Legislation

On a review of this file, it was determined that, while this matter was referred to us under the Breach Notification sections of the *Health Information Act*, because of the nature of the files, both the *Access to Information and Protection of Privacy Act* and the *Health Information* are applicable to and relevant to this review. Furthermore, provisions in the *Child and Family Services Act* are also applicable and relevant to the review.

Access to Information and Protection of Privacy Act

Under the Access to Information and Protection of Privacy Act, the following sections are relevant:

4. If a provision of this Act is inconsistent with or in conflict with a provision of another Act, the provision of this Act prevails unless the other Act expressly provides that it, or a provision of it, prevails notwithstanding this Act.

49.2.(1) The Information and Privacy Commissioner may conduct a review if he or she is of the opinion that a review is warranted in the circumstances.

Health Information Act

4. (1) This Act applies to all records containing personal health information that are in the custody or under the control of a health information custodian, except the following:

(a) a record referred to in subsection 71(1) of the Child and Family Services Act or any other record relating to the administration of that Act;

25.(1) Any right or power conferred on an individual by this Act, including any authority of an individual in respect of the collection, use or disclosure of personal health information about him or her, may be exercised, ...

(b) if the individual has not attained 19 years of age, but understands the nature of the right or power and the consequences of exercising the right or power, by that individual;

(c) if the individual has not attained 19 years of age and does not meet the requirement of paragraph (b), by a person who has lawful custody of, or lawful authority in respect of, the individual;

137. (1) If the Information and Privacy Commissioner is satisfied that a review is warranted in the circumstances, he or she may, without receiving a request under subsection 134(1), initiate a review of whether a health information custodian has collected, used or disclosed personal health information about one or more individuals in contravention of this Act.

Also of relevance are portions of the *Child and Family Services Act*

Child and Family Services Act

28 (7) Where a court makes a child protection order under paragraph (1)(c), the order may provide that the child's parent shall retain any right that the parent may have to give or refuse consent for medical care or treatment for the child.

47. (1) Where a child has been placed in the temporary custody of the Director, the Director has the rights and responsibilities of a parent in respect of the person of the child until

(a) the period of custody set out in the order expires; or

(b) a court, under paragraph 28(9)(c), discharges the order placing the child in the temporary custody of the Director.

(2) For the purposes of subsection (1), the rights of a parent in respect of the person of the child means only those rights in relation to the following:

(a) where and with whom the child will live;

(b) subject to an order made under subsection 28(7), consent for medical care or treatment for the child;

(c) the child's education;

(d) the child's social and recreational activities.

71. (1) Any information or record of information relating to a person is confidential where it is received, obtained or retained by any person

(a) under this Act or the regulations;

(b) in the exercise of his or her powers or in the performance of his or her duties under this Act or the regulations;

(c) who operates a child care facility or foster home respecting a child in the care of the child care facility or foster home; or

(d) who is employed by or retained on contract to provide services to a child care facility or foster home respecting a child in the care of the child care facility or foster home.

(2) Notwithstanding the *Access to Information and Protection of Privacy Act*, no person referred to in subsection (1) shall disclose or communicate any information or record of information described in subsection (1) to any person except

(a) where necessary or appropriate in the exercise of his or her powers or in the performance of his or her duties under this Act or the regulations;

(b) with the written consent of the person to whom the information or record relates, or where that person is a child,

(i) the person who has lawful custody of the child, or

(ii) the Director, where the child is in the temporary or permanent custody of the Director;

(c) where giving evidence in court;

(d) on the order of a court;

(e) to a person appointed to conduct an investigation under section 64 or 65;

(f) to the Minister, the Director, an assistant Director, a Child Protection Worker or an authorized person, at their request;

(g) to a peace officer, if the person believes on reasonable grounds that

(i) failure to disclose the information or record of information is likely to cause physical or emotional harm to a person or serious damage to property, and

(ii) the need for disclosure is urgent;

(h) where a disclosure or communication is required for the purposes of this Act or to protect a child;

(i) where necessary for the provision of care, counselling or education to the child;

(i.1) in accordance with subsection 57(4.1) of the Adoption Act;

(j) where, in the opinion of the Minister, the benefit of the release of the information would clearly outweigh any invasion of privacy that could result from the release; or

(k) where it is required for the purposes of this Act.

We have also taken into consideration recent amendments to the *Access to Information and Protection of Privacy Act* which have been passed by the Legislative Assembly of the Northwest Territories, but have not yet come into effect. We felt it important to comment on how these amendments will affect public bodies once they come into effect in the next several months. In particular:

- Section 35 will require the Information and Privacy Commissioner to made orders after completing a review, rather than simply making recommendations;
- Amendments require public bodies, including the Department of Health and Social Services, to notify the Information and Privacy Commissioner of material breaches of privacy;
- Individuals affected by a breach of privacy in which there is a real risk of significant harm to the individual as a result of the breach will have to be notified of the breach;

Issues

This review raised several preliminary issues:

1. Does ATIPPA or HIA apply in this review?
2. The importance of Bill 29: An Act to Amend the Access to Information and Protection of Privacy Act
3. The distinction between "privacy" and "confidentiality"

The review also raised the following main issues:

1. Is a review warranted under section 49.2 of ATIPPA?
2. Notification of affected individuals
3. Preventing the occurrence of similar breaches of privacy

Preliminary Matters

1. Does ATIPPA or HIA apply in this review?

Before I get into the analysis of the above noted issues, I do wish to raise a preliminary matter, which is that both "personal information" as described in the *Access to Information and Protection of Privacy Act* (ATIPPA) and also "personal health information" as described in the HIA have been lost in this case. More specifically, the information lost was a "social services file". This raises the question then as to which piece of legislation applies. HRHSSA indicated in its breach notification letters that it was notifying pursuant to the requirements set out in the *Health Information Act*. While I encourage all public bodies to report all significant privacy breaches to this office, I am not convinced that the HIA applies to this case so as to make that report mandatory, at least under the current legislation. Section 4(1)(a) of HIA states that the HIA does not apply to a record containing personal health information referred to in subsection 71(1) of the *Child and Family Services Act* or any other record relating to the administration of that Act. Section 71(1) of the *Child and Family Services Act* provides that any information or record of information relating to a person is confidential where it is received, obtained or retained by any person under that Act or the regulations and in the exercise of his or her powers or in the performance of his or her duties under the Act or the regulations. In this case, we are dealing with a social services file. I have not seen the contents of the reconstructed lost file but given that it was described by HRHSSA as a client's social services file and given the description of the information contained in the file, I am satisfied that most, if not all, of the information in the file would have been received, obtained or retained by a person performing their duties under the *Child and Family Services Act* or its regulations. Thus, as a result of the application of section 4(1)(a) of the *Health Information Act* , that legislation does not apply to the lost information. I think this is an unintended gap in the legislation, given that children in care should absolutely be entitled to the protections afforded by the HIA, including the

mandatory reporting of breaches affecting their personal information, just as the rest of NWT citizens are. The mandatory breach notification sections of the *Health Information Act* should apply when there has been a material breach as defined in the HIA.

That said, although section 4(1)(a) of the *Health Information Act* provides that that Act does not apply to child protection records, there is no similar provision in the *Access to Information and Protection of Privacy Act.* There is nothing in ATIPPA that excludes its application to social services files. Further, section 4 of ATIPPA states that if a provision of it is inconsistent with another piece of legislation, ATIPPA prevails unless the other Act expressly provides that it, or a provision of it, prevails notwithstanding ATIPPA. The *Child and Family Services Act* contains a notwithstanding ATIPPA clause with respect to a prohibition on disclosure and communication of information in section 71(2) but it does not include a notwithstanding clause with respect to the application of the remaining provisions in ATIPPA. Thus, in my view, except with regards to the prohibition on disclosure and communication as set out in section 71(2) of the *Child and Family Services Act*, the *Access to Information and Protection of Privacy Act* applies so as to provide protection for the personal information of clients under Part II of the Act which deals with the collection, use and disclosure of personal information.

2. The impact of Bill 29

This brings us to the impact that *Bill 29: An Act to Amend the Access to Information and Protection of Privacy Act* will have on privacy enforcement in the Northwest Territories. On October 25, 2018, notice of *Bill 29: An Act to Amend the Access to Information and Protection of Privacy Act* (Bill 29) was provided to the Legislative Assembly of the Northwest Territories. Bill 29 received royal assent on June 6, 2019. The Bill did not have a coming into force date but rather stated that it would come into force on a day or days to be fixed by order of the Commissioner. The Bill has not yet come into force but I expect that it will within the next few months. Bill 29 contains a number of dramatic

changes to ATIPPA. The first major amendment is that the Information and Privacy Commissioner (IPC) will now have order making power pursuant to section 35. This is in contrast to the current recommendation making power that the IPC has.

This review is being done under the old legislation and I will, therefore, be making recommendations only. I felt, however, that it was important to point out the important and significant change to the powers of the Information and Privacy Commissioner that Bill 29 will bring.

A second major amendment is the inclusion of mandatory breach notifications, similar to the breach notification provisions already existing in HIA. Bill 29 will require all public bodies to notify the Information and Privacy Commissioner of breaches of privacy with respect to personal information, as is currently required of health information custodians with respect to health information. Even though Bill 29 has not yet come into force, the concept of mandatory breach notification is hardly a new one and public bodies should be taking steps to ensure they are ready for breach notification when it becomes mandatory for all public bodies. Some public bodies have pro-actively started to do this. It is not necessary to wait for Bill 29 to come into force.

3. The distinction between "privacy" and "confidentiality"

I wish to raise one final preliminary matter, which is the distinction between "privacy" and "confidentiality". HRHSS labelled its investigation report as a “Breach of Confidentiality Report”. This is not the first time I have seen HRHSA and other public bodies refer to breaches of privacy as breaches of confidentiality. This is both incorrect and problematic. As set out by the Saskatchewan Office of the Information Privacy Commissioner (OIPC), privacy is the right of an individual to have some control over how his or her personal information (or personal health information) is collected, used, and/or disclosed. In the Northwest Territories, individuals' privacy is maintained through

ATIPPA and HIA. These laws establish individuals' right to privacy by setting out how public bodies can collect, use, and/or disclose personal information or personal health information. Confidentiality, on the other hand, is a far slimmer concept than privacy. Confidentiality is the duty to ensure information is kept secret. When an individual's rights are breached under ATIPPA or HIA, this is not simply a breach of confidentiality, it is a breach of privacy that brings along with it all the rights and powers conferred under ATIPPA and HIA. It is important for public bodies to understand the difference.

Discussion

1. Is a review warranted under section 49.2 of ATIPPA?

There is no question that the loss of a child and family services file would be a reportable breach under Bill 29. HRHSSA admits that personal information and personal health information was lost. However, there is no requirement for a breach report to be made to the IPC before she can undertake a review. Section 49.2 of the existing ATIPPA, allows the Information and Privacy Commissioner to undertake a review if information comes to her attention and she is satisfied that a review is warranted. For the reasons set out below, I felt that a review was warranted in this case.

First, I found the lack of urgency demonstrated by HRHSSA's actions concerning. Section 87 of the *Health Information Act*, which is the provision which prompted HRHSSA to report this breach, requires notice to be given “as soon as reasonably possible”. Similarly, the breach notification provisions of Bill 29 will require public bodies to provide breach notification "as soon as reasonably possible" after the public body knows or has reason to believe that the breach of privacy occurred and determines that the breach creates a "real risk of significant harm" to the individual. It is important to report breaches as soon as possible so that individuals affected can take steps to protect themselves from risk and harm.

Section. 49.9 (1) of Bill 29 requires notification to the IPC if the breach is "material". Individuals must be notified where there is a real risk of significant harm. While these provisions are not yet in effect, they are instructive and merit some discussion.

Section 49.9(2) of Bill 29 sets out that some of the factors that are relevant in determining whether a breach of privacy with respect to personal information under the control of a public body will be a material such that the breach should be reported to the IPC. These include:

(a) the sensitivity of the personal information;
(b) the number of individuals whose personal information is involved;
(c) the likelihood of harm to the individuals whose personal information is involved; and
(d) an assessment by the public body whether the cause of the breach is a systemic problem.

In this case, the lost file was described as containing "medical reports". It has long been established that medical information is some of the most sensitive personal information there is. In my opinion, any time personal health information is lost, the breach will almost always be a material one. Furthermore, the lost information includes investigation and incident reports which are often protected from disclosure under the *Child and Family Services Act*.

This breach appears to affect at least five people: the child, the foster parents and the biological parents. If the lost information is shared with unauthorized parties, it could negatively affect any or all of these individuals, as well as the Director of Child and Family Services, who is ultimately legally responsible for children in care. Also, as noted by the Alberta Information and Privacy Commissioner in her Investigation Report

H2015-IR-01 entitled "Privacy Breach Reporting in Alberta's Health Sector" (December 9, 2015):

> Health information is sensitive. A privacy breach involving health information can have significant impact on affected individuals and may cause hurt, humiliation and embarrassment, as well as pose a risk of identity theft or fraud. In some circumstances, a health information breach can also create risk to personal safety for those affected.

Finally, I am unsure whether HRHSSA did any in-depth assessment as to how this loss occurred. It is, therefore, impossible to determine whether the loss is part of a systemic issue. In the future I encourage the HRHSSA to do a far deeper dive into determining how the breach occurred so that systemic issues can be identified and addressed.

I find that the privacy breach was a material one.

With regards to notification to the affected individuals, section 49.10 (2) of Bill 29 sets out some of the factors relevant in determining whether a breach of privacy with respect to an individual's personal information creates a real risk of significant harm to the individual. These factors include:

(a) the sensitivity of the personal information; and
(b) the probability that the personal information has been, is being or will be misused.

As set out above, I have found that the lost information is sensitive. With regard to the possibility that the personal information may be misused, we know only that the information was "lost". HRHSSA has done no analysis to determine how the breach occurred so we cannot know who might find the file or when it might be found, if ever.

We must assume, therefore, that the file is accessible by unrelated third parties and that the personal information lost could be misused if found by an unauthorized party. Thus I find that the breach created a real risk of significant harm to the affected individuals.

Turning to the timing of the notification, the privacy breach occurred in February 2018. The foster parents were notified of the privacy breach on June 14, 2019. The Breach of Confidentiality Report was completed on June 19, 2018. My office was notified of the privacy breach on July 23, 2018. In correspondence to HRHSSA I asked why it took them four months to report the breach to my office. HRHSSA did not provide a reply to this question. To not respond to questions from the IPC is disrespectful and not helpful to the IPC's job of addressing privacy concerns in the public sector. To take approximately three months to notify the foster parents and four months to notify this office without explanation is contrary to good privacy practices and, in fact, contrary to law. As soon as the loss was confirmed, HRHSSA should have notified the correct parties. Without any submissions on this issue from HRHSSA, I must find that their notification was not completed "as soon as reasonably possible".

Further, I wrote to HRHSSA on August 29, 2018 and asked for their submissions in relation to this breach by September 30, 2018. They did not respond. I wrote again on October 26, 2018 and asked for a response by November 15, 2018. Again HRHSSA did not respond as requested but instead responded on November 19, 2018. In no way is ignoring correspondence from my office and ultimately taking approximately two and half months to reply appropriate. In no way do those actions convey that HRHSSA took this matter seriously. In the future I urge HRHSSA to respond to correspondence from this office in a timely manner, even if the response is to request more time. Simply ignoring this office is inappropriate.

Given these problems with HRHSSA's privacy breach notification and the inadequate steps taken by them to prevent future privacy breaches set out in more detail below, I

felt that a review was warranted in this case.

2. Notification of affected parties.

Section 49.10 of the *Health Information Act* requires a health information custodian to give notice to an individual if personal health information about the individual is lost and it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. We have already determined that the HIA does not apply. However, this section is, again, instructive with respect to best practices.

In this case, HRHSSA chose to only notify the foster parents of the child who was the subject matter of the lost social services file. This raises a number of issues.

First, when I asked whether the foster parents were notified that, in addition to their foster child's personal information, the missing records contained their own personal information as well, the response I received was that "the foster parents were notified of everything that went missing". However, HRHSSA also provided me with the notification letter to the foster parents. It simply says that what went missing was their foster child's "current social services file". It does not specify that their own information was in that file, as outlined in the Breach of Confidentiality Report which stated that the information breached contained "foster parent information".

In addition to "foster parent information", the Breach of Confidentiality Report stated that "parents information" was included in the lost social services file. From the information provided to this office, there is no indication that HRHSSA notified the child's biological parents that their personal information was also lost in this incident. It is very likely that the lost records contained very sensitive personal information of the child's natural parents. They also should have been notified of the loss.

I wish to also make some comments about HRHSSA's decision to notify the foster parents of the child but not the biological parents, the child or the Director of Child and Family Services. First, with respect to notifying the child, I have no knowledge of the age of the child, however I presume the child is under the age of majority given that she/he is in the care of foster parents. Unlike the HIA, both ATIPPA and Bill 29 are silent with respect to notification and minors. HIA contains a helpful section - section 25(1)(b) - which specifies that an individual's rights remain with a minor if that individual understands the nature of the right or power and the consequences of exercising the right or power by that individual. This is similar to the mature minor test. Essentially, if a child is mature enough to understand the nature and consequences of being subject to a privacy breach, that child should be informed.

Turning to notification of the biological parents, it appears that HRHSSA did not notify the biological parents of the child of the privacy breach. Rather, they notified only the foster parents. Again, both ATIPPA and Bill 29 are silent on this issue. Section 25(1)(c) of HIA helpfully states that the rights of a minor who does not understand the nature of those rights and the consequences of exercising them may be exercised by a person "who has lawful custody of, or lawful authority in respect of" the individual. What this and the common law state is that just because a child is in temporary custody does not mean that the biological parent would no longer be considered to have lawful custody of or lawful authority in respect of the child. The biological parents have a right to know about this privacy breach so long as there is not a court order preventing them from knowing such information.

In addition to the biological parents, there is also consideration to be given to the Director of Child and Family Services. Pursuant to section 47 of the Child and Family Services Act, where a child has been placed in the temporary custody of the Director, the Director has the rights and responsibilities of a parent in respect of a child, including the right to consent for medical care or treatment unless otherwise ordered by the court.

Here, as the child has foster parents, he/she has presumably been placed in the temporary or permanent custody of the Director. Unless there is a court order stating otherwise, the Director should also have been notified of the breach.

Finally, I should note that as the foster parents do not obtain legal rights of a parent with regards to a foster child, the notification to them was likely in breach of the ATIPP Act. This does not seem right in light of the fact that the foster parents have the day to day responsibility for the care and well-being of the child. However, as currently written, the law does not recognize this relationship. That said, they should have been notified of the breach insofar as the loss contained their personal information and in such circumstances would also have, by implication, been advised of the loss of information pertaining to the foster child.

3. Preventing recurrence

When the Information and Privacy Commissioner undertakes a review of a privacy breach, whether under the *Health Information Act* or the *Access to Information and Protection of Privacy Act,* and whether or not she determines that a breach occurred, she may recommend to the head of the public body that steps be taken to prevent the occurrence of future breaches or to avoid the possibility of a future breach. These recommendations may include, without limitation, implementing or increasing security safeguards within the public body.

In my correspondence to HRHSSA I asked for a description of the information management system for social services clients, including security measures to ensure privacy and confidentiality (administrative, physical and technical). The response I received was limited.

With respect to administrative measures for the protection of personal health information, HRHSSA referenced a privacy breach policy but did not provide me with a copy. I assume that they were referring to the Privacy Breach Policy which applies to all health information custodians by reason of a Minister's Directive issued in May, 2017. I could not find this policy on the HRHSSA website. Further, I could not find it on the Department of Health and Social Services' website.

Having a privacy breach policy is a good first step. However a policy is of little value if no one can find it so as to be guided by it. Given the extensive problems described above with their privacy breach notification steps, and assuming that the policy referred to is the Department of Health and Social Services' Privacy Breach Policy, it appears to be lacking proper depth in its notification provisions.

With respect to physical and technical safeguards, HRHSSA again did not provide me with a detailed response. That being said, I was able to deduce some information from the Breach of Confidentiality Report. HRHSSA indicated that paper-charts are kept in a file room that is opened at 8:30 each morning and re-locked at 16:30 each week day and that files identified as sensitive are locked in the Supervisor's office in the blue file cabinet. This is a start but it is not enough. It is unclear to me from HRHSSA's response whether the file room is monitored to prevent unauthorized access during the work day, nor who has access to the file room during the hours it is unlocked. Nor is it clear whether the Supervisor's Office is normally locked either during the work day or after hours. What makes one file sensitive and the next file not as sensitive? How is access to these rooms controlled? Is the blue file cabinet itself locked and, if so, by what means and who has access to it?

Child and Family Services records need to properly safeguarded from a physical perspective. Why are all child and family services files not locked and secure from unauthorized access?

The Report also details that there was no sign-in or sign-out process in place at the time the records were lost. A sign-in and sigh-out process was implemented only after it was discovered that the file was lost. This is troubling. An organization that has responsibility for social services, which collects extremely sensitive documents about individuals, should at minimum have a sign-in and sign-out process in place for all of its files containing personal information and personal health information. This requirement should be set out in policy. I am assuming that HRHSSA does not have such a policy as they did not share one with me, nor is there one on their website.

In terms of the steps it has taken to prevent a future similar privacy breach, HRHSSA reported that it has now implemented a file sign-in and sign-out procedure. It has also begun to implement mitigation recommendations from the "first report" (which was not provided to me), such as creating a database of current files and auditing them on a regular basis to ensure that all active files are accounted for. These are both positive first steps but they are not enough. In order to ensure that a breach like this does not occur again, I reiterate that policies are necessary and should be developed, implemented and enforced.

Conclusion and Recommendations

This was a serious and material breach of privacy. HRHSSA lost an entire file relating to a child in care. These files contain extremely sensitive personal information and personal health information. I therefore concluded that a review was warranted pursuant to section 49.2 of ATIPPA.

I found HRHSSA's actions in response to this breach troubling. It started with taking much too long to notify the affected party as well as this office of the privacy breach. It continued with HRHSSA twice failing to respond to correspondence from this office within the requested time frames. This was compounded by the problems noted in this

review with respect to notification of relevant parties. The scope of the investigation done to determine what happened and how it happened was lacking. And it ended with HRHSSA still not having taken reasonable steps following the privacy breach to prevent similar breaches in the future. I therefore make the following recommendations:

1. I recommend that HRHSSA review its policies and procedures to ensure that they appropriately distinguish between the concepts of privacy and confidentiality. I further recommend that training on this issue be provided to HRHSSA staff.

2. I recommend that HRHSSA clarify with the foster parents that their personal information was included in the information which was lost. HRHSSA should be as specific as possible in detailing what personal information was lost.

3. I recommend that HRHSSA notify the biological parents that their personal information was also lost. HRHSSA should be as specific as possible in detailing what personal information was lost.

4. I recommend that HRHSSA notify the affected child if it is determined that the child understands the nature of his/her rights and the consequences of exercising them.

5. I recommend that HRHSSA notify the Director of Child and Family Services of this privacy breach.

6. I recommend that HRHSSA review its Privacy Breach Policy with respect to how it covers notification of privacy breaches and update it accordingly. The policy should be publicly posted to the HRHSSA website.

7. I recommend that HRHSSA develop a policy that addresses the physical and technical safeguards required for the storing of sensitive social services client files (if it has not already done so). The policy should then also be posted to the HRHSSA website.

8. I recommend that HRHSSA keep a record of this privacy breach and any corrective measures taken as a result. A log of all privacy incidents should be developed. The log should also be reviewed regularly so as to identify systemic or regularly occurring issues and to facilitate steps to be taken to address such problems.

Elaine Keenan Bengts
Information and Privacy Commissioner