ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2010-ND-011

Case File #P1707

November 30, 2010

Speech-Language Pathologist (SLP) Jillian Rowsell

I. Introduction

[1] On October 28, 2010, I received a report from Speech Language Pathologist (SLP) Jillian Rowsell ("Ms. Rowsell") of an incident involving the loss of personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to individuals as a result of the incident, and therefore I require that Ms. Rowsell notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] Under s. 34.1 of the *Personal Information Protection Act* (PIPA), an organization having personal information under its control must, without unreasonable delay, notify me of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

[3] Section 37.1 of PIPA authorizes me to require an organization to notify individuals to whom there is a real risk of significant harm as a result of an incident. It states:

> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
>
> (a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

(2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of signification harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

(4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), and

(c) to satisfy terms and conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

[4] PIPA applies to organizations, defined in section 1(1)(i) of PIPA as follows:

1(1) (i) "organization" includes

(i) a corporation,

(ii) an unincorporated association,

(iii) a trade union as defined in the *Labour Relations Code*,

(iv) a partnership as defined in the *Partnership Act*, and

(v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

[5] I have jurisdiction in this matter because Ms. Rowsell is an "organization" as defined in section 1(1)(i) of PIPA, and the information at issue in this incident qualifies as "personal information" as defined in section 1(1)(k). The services provided by Ms. Rowsell are, for the most part, services provided to children who qualify for Program Unit Funding, which is provided to schools through the Government of Alberta. As such, these services fall under the *Freedom of Information and Protection of Privacy Act* ("FOIP"), and Ms. Rowsell is considered an employee under section 1(e) of FOIP. However, services provided to one client were paid for privately under Alberta Blue Cross and therefore PIPA applies.

[6] In considering whether to require Ms. Rowsell to notify the affected individual, I am mindful of PIPA's purpose and legislative principles and the relevant circumstances surrounding the reported incident.

III. Background

[6] On October 28, 2010, I received a written report from Ms. Rowsell describing an incident involving the loss of personal information.

[7] On November 1, 2010, my Office contacted Ms. Rowsell to request that she provide additional information concerning the incident, in order for me to determine whether to require her to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls and email correspondence between November 1, 2010 and November 8, 2010.

[8] The circumstances of the incident reported to me are as follows:

- On October 26, 2010, at 11:36 a.m., Ms. Rowsell's security alarm was triggered by an intruder break-in. All of the doors and windows had been locked and the alarm system had been armed. The intruder physically removed a window to get in and then broke the lock on the door.

- Ms. Rowsell was contacted by her security company and discovered approximately one hour after the break-in, while performing a walk-through with the Calgary Police, that two laptops had been stolen from the office. Given the triggering of the alarm system, the theft appeared to be a "dash and grab", where the laptops were the most obviously valuable items in the office.

- One of the stolen laptops contained an external hard drive with the personal information of approximately 50 speech pathology clients. All of Ms. Rowsell's

affected clients were children under six years old, most with special needs. All but one child qualified for Program Unit Funding, which is provided to schools through the Government of Alberta. The speech pathology services for one child with special needs were privately paid for through Alberta Blue Cross, and therefore PIPA applies.

- Ms. Rowsell explained that the external hard drive with client information was normally stored in a locked filing cabinet in the office, but as the files had been worked on earlier on the morning of October 28, 2010, with the intent of additional work later that day, the external hard drive was still attached to the laptop at the time of the theft.

- The lost information about the privately funded client included: the name of the child, the parents' names, the child's date of birth, home address and contact numbers, name of school, speech-language pathology session summaries, the speech-language pathology portion of an individualized program plan update and a speech-language pathology report. The information of the affected publicly funded clients was similar.

- The laptop did not contain any financial information, social insurance numbers or Alberta Health Care numbers.

- Following the break-in, Ms. Rowsell replaced the broken lock and added additional alarm sensors. Ms. Rowsell states that when a replacement laptop is purchased, it will be encrypted, and Ms. Rowsell will continue her practice of locking the remaining personal information on an external hard drive in a filing cabinet.

- Ms. Rowsell sent notification letters to the parents of all of her affected clients within a few days of the theft. The notification letters included:
    - A description of the circumstances of the loss;
    - The date on which the loss occurred;
    - A description of the personal information involved in the loss;
    - A description of the steps that were taken to reduce the risk of harm; and
    - Contact information for an individual who could answer, on behalf of Ms. Rowsell, questions about the loss.

IV. Is there a real risk of significant harm to the individual as a result of the incident?

[9] Pursuant to section 37.1 of PIPA, I have the power to require Ms. Rowsell to "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure." In determining whether or not to require Ms. Rowsell to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

[10] In order for me to require that Ms. Rowsell notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to her client as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[11] In this case, the personal information at issue is about a special needs child and its parents, including contact information, date of birth, school, and limited medical information regarding speech pathology treatment. The information does not include any unique identifiers such as Alberta Health Care numbers or social insurance numbers. An important factor in this case is that the affected individual is a child under six years old, and is therefore, in my view, a vulnerable individual who requires a higher degree of protection.

[12] There is sufficient information available regarding the affected child that a person with nefarious purposes could concoct a scenario to lure the child away. For example, a person could pose as a substitute speech pathologist and using information about the child's treatment, the child's parents, the child's school etc. could convince a young child to leave with him or her, or otherwise manipulate the child to cause harm. This, in my view, is a significant harm.

[13] In order for me to require Ms. Rowsell to notify the affected individual, however, there must also be a "real risk" of harm to the individual as a result of the incident. This standard does not require that harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. Further, there must be a cause and effect relationship between the incident and the possible harm.

[14] In this case, Ms. Rowsell's laptop was stolen, which clearly indicates it was taken for an improper purpose. At this time, no information is known as to what that improper purpose may have been. Child abduction, or even using stolen personal information to manipulate a child is not a certainty or even "high risk", but it is a real risk.

[15] In deciding whether there exists a "real risk" of harm in this case, I considered that one of the affected individuals is a young, special needs child and is more vulnerable to manipulation using the personal information available than the average person.

[16] Given the information reported by Ms. Rowsell, I have decided that there is a real risk of significant harm to the affected individual as a result of this incident. I have based my decision on the following factors: the affected individual is a vulnerable, special needs child and the type of information involved could be used for improper purposes to lure or manipulate a child, which is a significant harm.

V. Decision

[17] Based on the information reported to me by Ms. Rowsell, I have concluded there is a real risk of significant harm to the affected individual as a result of this incident and I require Ms. Rowsell to notify the affected individual in accordance with section 19.1 of

the *Personal Information Protection Act Regulation.* Section 19.1(2) states that notification may be given to an individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances. Clearly, it would be unreasonable to provide notification to a young, special needs child who is affected by this breach, and as such, notification to the parents is sufficient.

[18] I understand Ms. Rowsell has already notified the parents of all of her affected clients, not just the client who falls under PIPA, by way of letters mailed on October 28 and October 29, 2010. I commend Ms. Rowsell for taking immediate steps to notify the parents of all of her affected clients, and for agreeing to encrypt her laptop in the future; however, I note that had the stolen laptop been encrypted in the first place, notification would not have been required.

Frank Work, Q.C.
Information and Privacy Commissioner