ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-004

AARC SOCIETY
operating as ALBERTA ADOLESCENT RECOVERY CENTRE

February 7, 2011

(Case File #P1742)

I. Introduction

[1] On December 16, 2010, I received a report from the Alberta Adolescent Recovery Centre ("AARC") of an incident involving the unauthorized access to 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 AARC notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] Under section 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 significant 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] AARC reported that the information at issue in this incident consists of twenty-four client names, addresses, Alberta Health Care Numbers, telephone numbers of the clients' parents, medical histories which include allergies and medications currently prescribed, and individual photographs of these clients. AARC further stated that these clients and their families are treated by AARC's clinical staff which includes registered psychologists, clinical counsellors, family therapists and peer counsellors.

[5] Initially, after receiving AARC's report and reviewing the information involved in this incident, I considered whether or not Alberta's *Health Information Act* (HIA) applied in this case as PIPA does not apply to health information as defined in the HIA pursuant to section 4(3)(f) of the Act.

[6] The HIA applies to "health information" in the custody or control of "custodians".

[7] Health information is defined in section 1(1)(k) of the HIA as follows:

> 1(1)(k) "health information" means one or both of the following:
>
> (i) diagnostic, treatment and care information;
>
> (ii) registration information;

[8] A "custodian" includes, among other things, "a health services provider who is designated in the regulations as a custodian, or who is within a class of health services providers that is designated in the regulations for the purpose of this subclause" [1(1)(f)(ix)]; "the Department" (Alberta Health and Wellness) [1(1)(f)(xii)]; and a regional health authority [1(1)(f)(iv)].

[9] The information at issue in this incident is not health information to which the HIA applies as the clinical staff of AARC are neither custodians, nor affiliates to a custodian in providing these services.

[10] As the AARC clinical staff are neither custodians, nor affiliates to a custodian, in providing long-term treatment services, the HIA does not apply in this case.

[11] I next considered whether or not PIPA applies in this case, given that AARC is a non-profit organization incorporated under the *Societies Act* of Alberta.[1]

[1] Alberta Corporate Registry System - AARC Society (Alberta Adolescent Recovery Centre), Corporate Access Number: 504030438

[12] Section 56(1)(b)(i) of PIPA defines "non-profit organization as follows:

> (b) "non-profit organization" means an organization
>
> (i) that is incorporated under the *Societies Act* or the *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act* …

[13] Pursuant to sections 56(2) and (3), PIPA does not apply to a "non-profit organization" except in the case of personal information that is collected, used or disclosed in connection with any commercial activity. These provisions state:

> 56(2) Subject to subsection (3), this Act does not apply to a non-profit organization or any personal information that is in the custody or under the control of a non-profit organization.
>
> 56(3) This Act applies to a non-profit organization in the case of personal information that is collected, used or disclosed by the non-profit organization in connection with any commercial activity carried out by the non-profit organization.

[14] In this case, AARC is an organization incorporated under the *Societies Act* and so the provisions of PIPA apply only when AARC collects, uses or discloses personal information in connection with a "commercial activity".

[15] Commercial activity is defined in section 56(1)(a) of PIPA as follows:

> (a) "commercial activity" means
>
> (i) any transaction, act or conduct, or
>
> (ii) any regular course of conduct, that is of a commercial character and, without restricting the generality of the foregoing, includes the following:
>
> (iii) the selling, bartering, or leasing of membership lists or of donor or other fund-raising lists;
>
> (iv) the operation of a private school or an early childhood services program as defined in the *School Act*;
>
> (iv) the operation of a private college as defined in the *Post–secondary Learning Act*;

[16] In deciding whether the information at issue is connected to a commercial activity, I considered that the purpose of AARC's program is to provide assessment, treatment and aftercare services to adolescents and their families.

[17] AARC provides these services in exchange for a fee, which is established based on the family's income; that is, AARC reviews each family's financial situation and assesses fees based on their ability to pay.

[18] In my view, services provided by AARC qualify as a "commercial activity" under section 56(1)(a) of PIPA. Therefore, pursuant to section 56(3), PIPA applies to AARC and the information at issue in this incident.

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

III. Background

[20] On December 16, 2010, I received a written report from AARC describing an incident involving the unauthorized access to personal information.

[21] On December 20, 2010, my Office contacted AARC by telephone to request that it provide additional information concerning the incident, in order for me to determine whether to require AARC to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided by telephone and email correspondence on December 20 and 21, 2010.

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

- An AARC staff member was "on call" the night of December 12, 2010;
- An AARC binder containing client data and information was stored in a staff member's locked vehicle;
- After 9:00 p.m., the staff member witnessed an unauthorized individual driving away with his vehicle;
- The binder contained twenty-four paper files which included clients' names, addresses, Alberta Health Care Numbers, parents' telephone numbers, medical histories referring to allergies and medications currently prescribed, and individual photographs of these clients;
- The affected clients are between 12 to 20 years of age;
- The staff member immediately reported the incident to the Calgary Police Service and senior staff of AARC;

- AARC determined there was a "real risk of significant harm" to individuals as a result of this incident;
- AARC reported the incident to my Office on December 16, 2010 and directly notified the parents of the affected clients on December 21, 2010;
- AARC examined its safeguard measures for the protection of clients' personal information. The organization met with all staff to discuss the incident and together they revised AARC's procedures to protect client information.

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

[23] Pursuant to section 37.1 of PIPA, I have the power to require AARC 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 AARC to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

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

[25] In this case, the personal information at issue is of moderate to high sensitivity as it includes clients' names, addresses, Alberta Health Care Numbers, telephone numbers of the clients' parents, medical histories which includes allergies and medications currently prescribed, and individual photographs of these clients. I also note that the information is that of young adolescents seeking treatment for addictions.

[26] In my view, the personal information in AARC's binder could be used to cause significant harm to these individuals in the form of harassment, distress and humiliation.

[27] AARC also noted that the type of harm that could result from the unauthorized access to or disclosure of this information is identity theft, risk of harassment, hurt, humiliation, and damage to reputation.

[28] In order for me to require AARC to notify its clients, 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.

[29] Given the information reported by AARC, I have decided that there is a real risk of significant harm to individuals as a result of this incident. In deciding this, I considered the circumstances surrounding the loss of the personal information. The fact that the personal information was in a locked vehicle that was taken by an individual intentionally committing a criminal act suggests that it is likely that the culprit would have no compunction about using the personal information for purposes such as identity theft or to cause distress and humiliation to the affected individuals. In addition, the information is readily accessible in the form of paper records rather than electronic records with password protection and encryption. Given the sensitivity of the personal information and that the information is readily accessible to anyone who may find the information, I find there is a real risk of significant harm to individuals in this case.

V. Decision

[31] I understand AARC has already notified the parents of the affected clients by way of a meeting with AARC's senior board members on December 21, 2010. However, section 37.1(1)(a) of PIPA gives me the power to require that AARC notify individuals "in a form and manner prescribed by the regulations". Therefore, I require AARC to notify the parents of the twenty-four clients in accordance with section 19.1 of the *Personal Information Protection Act Regulation*, if it has not already done so.

Frank Work, Q.C.
Information and Privacy Commissioner