ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2010-ND-010

Ms. Sharon Ashton

December 15, 2010

(Case File #P1717)

I. Introduction

[1] On November 3, 2010, I received a report from Ms. Sharon Ashton ("the Psychologist") who is a registered psychologist and sole proprietor. The Psychologist shares an office with two other psychologists at a family health centre located in Calgary, Alberta. The Psychologist reported 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 the Psychologist 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 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] Initially, after receiving the Psychologist's report and considering 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 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 Psychologist is neither a custodian, nor an affiliate to a custodian in providing these services. The Psychologist advised that all her clients voluntarily come to her for counselling services and privately remunerate the Psychologist for these services.

[10] As the Psychologist is neither a custodian, nor an affiliate to a custodian, in providing counselling services, the HIA does not apply in this case.

[11] Instead, I have jurisdiction in this matter because the Psychologist 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).

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

III. Background

[13] On November 3, 2010, I received a written report from the Psychologist describing an incident involving the unauthorized access to personal information.

[14] On November 9, 2010, my Office was advised that the Psychologist was out of the country and expected to return on November 14, 2010. On November 16, 2010, the Psychologist contacted my Office and provided further information about the incident by telephone and correspondence.

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

- October 9 (Sat), 2010: The Psychologist shares an office with two other psychologists. On October 9, the Psychologist reported that one of the other psychologists noticed that their shared file cabinet would not open and that the cylinder lock was missing. The other psychologist assumed that the Psychologist had had problems with the file cabinet. The Psychologist stated that she and the other psychologists lock the file cabinet on a daily basis but do not lock the door to their office as the family health centre is locked after business hours and secured with an alarm system.

- October 10 (Sun): Psychologist's Office closed.

- October 11, (Mon): Psychologist's Office closed for statutory holiday. The other psychologist contacted the Psychologist later that evening. She asked the Psychologist if she had tinkered with the file cabinet as the cabinet lock was missing. The Psychologist told the other psychologist that she had not tampered with the cabinet lock. Consequently, both psychologists decided that they would check the file cabinet the following morning.

- October 12, (Tues): Both psychologists examined the file cabinet. They found that the cylinder lock was missing and the cabinet drawers were inoperative. The psychologists advised the manager of the family health centre of the incident and telephoned the Calgary Police Service (CPS). Subsequently, the Psychologist on behalf of both psychologists, submitted an on-line report to CPS. She also telephoned a locksmith to open the file cabinet drawers and fix the cabinet lock. The locksmith was unable to come to the office until the following day.

- October 13 (Wed): The manager of the family health centre noticed during opening hours that a chair was positioned in front of the psychologists' file cabinet. The manager reported her observations to the psychologists. When the Psychologist arrived at the office, she examined the file cabinet and its contents. She discovered that the drawers to the file cabinet were operative and that some of her client files appeared to "have been moved because they sat higher in the drawer than other files". Subsequently, the other psychologist examined her client files and determined that "nothing appeared to be missing". Both psychologists advised a third psychologist, with whom they shared office space, of the incident and asked her if she had stored her client files in the file cabinet. The third psychologist reported that she had no files in the office file cabinet.

- The Psychologist stated that there was no theft or damage done to her office with the exception of the tampered file cabinet and the other offices in the family health centre were undisturbed.

- The Psychologist advised that she has reviewed her client files that were in the file cabinet as well as her former client files for potential risk to clients by a third party. The Psychologist reported that to the best of her ability she has determined that there are no discernable risks to her clients by a third party.

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

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

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

[18] In this case, the personal information at issue is of moderate to high sensitivity as it includes clients' names, addresses, and of most significance, the Psychologist's counselling session notes which contain the clients' feelings, thoughts and behaviours as recorded by the Psychologist.

[19] My Office reviewed copies of a select number of counselling session notes from the Psychologist's client files. A description of these files is outlined below:

- Twenty four paper record file folders
- All files contain client names, addresses and counselling session notes
- Counselling session notes do not include diagnostic/assessment information. The notes are handwritten and document information provided by the Psychologist, current concerns of the client are summarized and behavioural changes since the previous counselling session are documented.

[20] The Psychologist made the following statement about the incident:

> *Nothing appears to be missing from these files in whole or in part. It is possible that a file or files could have been read, however, none were out of order. There was no apparent damage or vandalism to the contents of the files.*
>
> *The nature of the notes contained in the files would not have been damaging for the individuals involved if read by an unauthorized individual. The only concern would be embarrassment about attending counselling.*

[21] In my view, the personal information in the Psychologist's client files could be used to cause significant harm to individuals in the form of distress, anxiety and embarrassment.

[22] In order for me to require the Psychologist to notify her clients, however, there must also be a "real risk" of harm to those individuals as a result of the incident. This standard does not require that harm will certainly result from the incident, but the likelihood that it would 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.

[23] Although it is not known whether or not the unauthorized individual peered through the Psychologist's clients and/or recorded the contents, it is the case that an unauthorized individual had access to the files. Further, based on what appears to be repeated attempts over the course of days to open the locked file cabinet, it is reasonable to assume the unauthorized individual deliberately intended to access personal information in the Psychologist's client files.

[24] Therefore, given the information reported to me by the Psychologist, I have decided that there is a real risk of significant harm to individuals as a result of this incident. I have based my decision on the following factors:

1. The counselling session notes contain information about the clients' private feelings and thoughts and behaviours (and clients' family members) which could be used to cause distress or anxiety to the affected individuals.

2. Although the client files were all accounted for by the Psychologist it is nonetheless the case that an unauthorized individual accessed them for an unknown, potentially nefarious, purpose.

3. The Psychologist's office was the only office amongst the other offices at the family health centre that was accessed by the unauthorized individual, and the access occurred on two separate occasions. As noted above, the unusual circumstances of this incident suggest that information in the client files might have been the target of the unauthorized individual's actions, and that such access was committed with the intent to cause harm.

V. Decision

[25] Based on the information reported to me by the Psychologist, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require the Psychologist to directly notify her clients by telephone or in person (at her discretion) in accordance with section 19.1 of the *Personal Information Protection Act Regulation*, and confirm in writing to my Office that it has done so on or before December 31, 2010 or such other date as I may specify.

Frank Work, Q.C.
Information and Privacy Commissioner