ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-12

Leading Edge Physiotherapy

August 23, 2013

(Case File #P2248)

I. Introduction

[1] 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.

[2] On February 4, 2013, Leading Edge Physiotherapy (the Organization) provided notice of an incident involving the loss of personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to the affected individuals as a result of the incident. I require the Organization to notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[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] 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] The Organization is a corporation registered and operating in Alberta. The incident involved the theft of a hard drive from the Organization's premises that contained a backup copy of patient files. The incident involved both private patients of the Organization and patients treated on behalf of Alberta Health Services (AHS).

[6] The Organization reported the incident involved the following information contained in its patient files:

- patient information:
    - name,
    - address,
    - telephone number,
    - gender,
    - date of birth,
    - employment information (place and occupation),
    - Alberta Health Care Number (AHC Number),
    - medical information (family physician, medical history, conditions, and current medications),
    - benefits coverage, and
    - patient signature.
- physiotherapy treatment information (medical assessment, notes and diagnosis), and,
- the patient's physician referral note.

[7] The following information, taken at the time of patient registration, may have also been involved:

- worker's compensation claim information (date of accident, claim number, and employer)
- insurance policy number
- social insurance number (SIN)
- credit card number.

[8] Due to the nature of the information involved in this incident, I considered whether or not Alberta's *Health Information Act* (HIA) applied in this case. Under section 4(3)(f), PIPA does not apply to "health information" as defined in HIA to which that Act applies.

[9] 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;

[10] The HIA applies to "health information" in the custody or control of a "custodian" as defined by section 1(1)(f) of HIA. It also applies to affiliates, in relation to custodians, that are employed by the custodian or who perform a service for the custodian under a contract or agency relationship under section 1(1)(a) of HIA.

[11] AHS is a "custodian" under section 1(1)(f)(iv) of HIA. The Organization reported that some information involved in the incident pertained to clients of AHS that the Organization provided services to on behalf of AHS.

[12] Based on the information provided by the Organization, the Organization may be an "affiliate" under section 1(1)(a) of HIA with respect to patient information concerning clients of AHS that also met the definition of "health information." The health information of those patients would be under the jurisdiction of HIA. However, patient information concerning private clients who voluntarily came to the Organization for services would be under the jurisdiction of PIPA.

[13] I have jurisdiction under PIPA with respect to the information provided to the Organization by private clients because it is an "organization" as defined in section 1(1)(i) of PIPA and the information at issue is "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[14] On February 13, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization between February 13 and July 19, 2013.

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

- On February 3, 2013, the Organization's office was broken into.
- An unencrypted external hard drive containing patient files, as well as some money, was stolen from a locked safe.

- The unencrypted hard drive held backup copies of 2049 patient files.
- The files were for patients who received physiotherapy services between 2003 and 2008.
- The Organization reported the theft to the Royal Canadian Mounted Police.
- The Organization did not notify the affected individuals about the incident.

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

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

[17] Pursuant to section 37.1 of PIPA, I have the power to 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." In determining whether or not to require the Organization to notify the affected individuals, I must consider if there is a "real risk of significant harm" to the affected individuals as a result of the incident.

[18] In order for me to require that the Organization notify the affected individuals, there must be some harm – some damage or detriment or injury – that could be caused to those affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.

[19] The Organization reported the type of harm that could occur to the affected individuals as a result of the incident is identity theft or financial harm.

[20] In my view, this incident involves highly sensitive personal information. The information at issue includes names, addresses, dates of birth, medical information, AHC Numbers, and signatures. For some of the affected individuals it also includes insurance or WCB information, SINs, and credit card numbers. Unauthorized access to the personal information involved in this incident could result in identity theft, fraud, hurt, humiliation, and damage to reputation to the affected individuals. In my view, these are significant harms.

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

[22] The Organization recognized that the information was highly sensitive. However, it reported it did not believe there was a real risk that identity theft or financial theft would occur as a result of this incident for the following reasons:

- Additional items containing personal information that could have been taken during the robbery were left behind. These included paper patient files, a point-of-sale terminal, credit card receipts, cheques, and laptops.
- It appeared this was a crime of opportunity and not an attempt to target personal information. For example, the thieves were trying to steal a television when the theft was interrupted.

[23] Breach notification decisions P2010-ND-005, P2010-ND-11, P2011-ND-14, P2011-ND-025, and P2011-ND-028 also involved the theft of unencrypted hard drives containing highly sensitive personal information. The hard drives were not recovered. In each of these cases, the former Commissioner determined there was a real risk of significant harm (identity theft and fraud) to the affected individuals.

[24] Based on the above, I have decided there is a real risk of significant harm to the affected individuals as a result of this incident. The sensitivity of the personal information involved in the incident together with the fact that the hard drive, which was unencrypted, was taken by an individual with nefarious intent and not recovered are significant factors in reaching my decision.

V. Decision

[25] I require the Organization to notify the affected individuals, whose information is under the jurisdiction of PIPA, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

[26] The Organization submitted direct notification based on the last known address of affected individuals would not be reasonable in these circumstances because the addresses may not be up to date due to the age of the information involved. The Organization suggested the following method to indirectly notify the affected individuals:

a) post a notice in accordance with the Regulation in the local weekly newspaper, the St. Albert Gazette, for three consecutive Saturdays.

[27] I agree with the Organization that direct notification would not be reasonable in the circumstances for the reason it provided. I require the Organization to confirm in writing to my Office that it has indirectly notified the affected individuals as set out in paragraph [26] on or before September 20, 2013.

Jill Clayton
Information and Privacy Commissioner