



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	The Children's Cottage Society of Calgary (Organization)
Decision number (file number)	P2019-ND-140 (File #012209)
Date notice received by OIPC	February 28, 2019
Date Organization last provided information	February 28, 2019
Date of decision	August 15, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	<p>Pursuant to section 56(2), PIPA "does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization", except in the case of personal information that is collected, used or disclosed in connection with any commercial activity.</p> <p>"Non-profit organization" is defined in section 56(1) to mean an organization "that is incorporated under the <i>Societies Act</i> or the <i>Agricultural Societies Act</i> or that is registered under Part 9 of the <i>Companies Act</i>."</p> <p>In this case, the Organization reported that it is registered under the <i>Societies Act</i> and is a charitable agency established to prevent harm and neglect to children through providing support services, respite programs and crisis nurseries. The Organization employs over 140 full time and part time employees to carry out its functions. The personal information that was the subject of the breach was in respect of these employees.</p> <p>To the extent the personal information at issue was collected in connection with any commercial activities of the Organization, PIPA applies.</p>

<p>Section 1(1)(k) of PIPA “personal information”</p>	<p>The incident involved “Salaries and benefit plan details, calculations and premiums for all Society staff as well as vacation and sick time accrual and usage details for all Society staff.”</p> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
<p>DESCRIPTION OF INCIDENT</p>	
<p><input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure</p>	
<p>Description of incident</p>	<ul style="list-style-type: none"> • On February 5, 2019, a (now former) employee of the Organization emailed the information at issue to her personal email address. • The employee had authorized access to the information during her employment. • The incident was discovered on February 13, 2019, when another employee was reviewing the former employee’s emails and found confidential information had been sent to the former employee’s personal email address.
<p>Affected individuals</p>	<p>The incident affected 140 individuals.</p>
<p>Steps taken to reduce risk of harm to individuals</p>	<ul style="list-style-type: none"> • On February 15, 2019, the Organization sent a cease and desist letter requesting the former employee immediately stop any use, possession, copying, accessing or viewing of the information. The Organization also requested that the former employee permanently delete and destroy any and all confidential information. • On February 17, 2019, the former employee confirmed she had taken the above measures and provided an executed statutory declaration confirming that she had "permanently deleted and destroyed any and all confidential or personal information, documents, records or materials of the Society, in both paper and electronic form, including but not limited to the personal information of any current or former employees, agents or contractors". • The Organization will continue to investigate and review policies and procedures to identify any further measures it considers appropriate to help mitigate against the risk of future similar incidents.
<p>Steps taken to notify individuals of the incident</p>	<p>Affected individuals were notified by emailed letter on February 22, 2019.</p>

REAL RISK OF SIGNIFICANT HARM ANALYSIS

<p>Harm Some damage or detriment or injury that could be caused to 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.</p>	<p>The Organization reported “It is possible that the information disclosed as part of this breach may be provided to unauthorized persons or organizations or its disclosure could be embarrassing [sic] or sensitive.”</p> <p>In my view, a reasonable person would consider that the employment information at issue, including salaries, could be used to cause the significant harms of hurt, humiliation and embarrassment.</p>
--	---

<p>Real Risk The likelihood that the significant harm 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.</p>	<p>The Organization reported:</p> <p style="padding-left: 40px;"><i>There is a risk of harm resulting from the breach. The disclosure was discovered 8 days after the breach occurred. All ...employees are affected by this breach. However, there are mitigating factors which reduce the risk. The nature of the information, while personal information, is not highly sensitive. SS was authorized in her role to view this information so its disclosure to her would not be new. There is no evidence of any malicious intent or purpose. To [the Organization’s] knowledge, the information was only exposed to SS. In addition, [the Organization] has taken steps to mitigate further against any risks, as described below.</i></p> <p>In my view, the likelihood of harm resulting from this incident is reduced because of the steps the Organization took to obtain the statutory declaration confirming the information was deleted. However, I am concerned that while the Organization said there “is no evidence of any malicious intent or purpose”, it did not report what the former employee’s purpose was. The information was exposed for 8 days before being discovered. The text of the statutory declaration does not appear to confirm that the information was not already used or forwarded.</p>
--	--

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

A reasonable person would consider that the employment information at issue, including salaries, could be used to cause the significant harms of hurt, humiliation and embarrassment.

The likelihood of harm resulting from this incident is reduced because of the steps the Organization took to obtain the statutory declaration confirming the information was deleted. However, I am concerned that while the Organization said there “is no evidence of any malicious intent or purpose”, it did not report what the former employee’s purpose was. The information was exposed for 8 days before being discovered. The text of the statutory declaration does not appear to confirm that the information was not already used or forwarded.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand affected individuals were notified by emailed letter on February 22, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner