



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	MEM Psychological Services Inc. (Organization)
Decision number (file number)	P2020-ND-170 (File #016780)
Date notice received by OIPC	March 16, 2020
Date Organization last provided information	March 17, 2020
Date of decision	December 3, 2020
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”	The Organization operates in Alberta and is an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	The incident involved all or some of the following information: <ul style="list-style-type: none">• name, and• email address. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On March 16, 2020, the Organization sent an email to clients informing them how to access virtual services. The email was sent to 41 clients without blind copying client names and email addresses.• A second email containing a consent form for virtual services was then sent to 11 clients without blind copying client names and email addresses.

	<ul style="list-style-type: none"> • The incident was discovered the same day, when a client forwarded one of the emails to a Psychologist, alerting her to the breach. • The Organization subsequently identified a third occasion where an email was sent to 41 additional names and email addresses, without the use of blind carbon copy. • On March 17, 2020 the Organization submitted a second breach report to the OIPC regarding the third incident.
Affected individuals	The incident affected 93 individuals.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Notified affected individuals and asked them to destroy the email. • Developed a new training and supervision protocol for front desk staff. • Changed protocol so that only one supervisor manages the reception email. • Developed a new policy for front desk employees that prohibits the transmission of emails to multiple parties. • Terminated the reception staff who inadvertently sent the three emails.
Steps taken to notify individuals of the incident	Affected individuals were notified by email, followed by a telephone call, on March 16 and 17, 2020.
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:</p> <p style="text-align: center;"><i>People would have had their identity distributed to others who receive services at our clinic. Thus I would expect that their confidence in our ability to provide a safe place to receive service would be compromised. I could anticipate a sense of embarrassment [sic] for the people affected. I would imagine that there could be ongoing concerns about other breaches that could occur. It is possible that someone on the list knew someone else, and thus that could create difficulties within interpersonal relationships. It is possible that people on the list could begin emailing others.</i></p> <p>I agree with the Organization’s assessment. A reasonable person would consider the contact and health information at issue (individuals are seeing a Psychologist) could be used to cause the harms of hurt, humiliation and embarrassment as well as damage to reputation or relationships. Furthermore, email addresses could be used for phishing purposes, increasing</p>

	vulnerability to identity theft and fraud. These are significant harms.
<p>Real Risk</p> <p>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="text-align: center;"><i>What was shared was the names and email addresses of the clients on the list. We have asked all people who received the email to destroy it. Everyone with whom we spoke took the matter seriously and agreed to destroy [sic] the original email.</i></p> <p>In my view, a reasonable person would consider that the likelihood of harm is decreased because the breach did not result from malicious intent, but rather human error and the unintended recipients agreed to destroy the information. However, the risk is increased given the nature of the information at issue, the number of unauthorized recipients, and the potential for personal or professional relationships between the recipients and affected individuals.</p>
DECISION UNDER SECTION 37.1(1) OF PIPA	
<p>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.</p> <p>A reasonable person would consider the contact and health information at issue (individuals are seeing a Psychologist) could be used to cause the harms of hurt, humiliation and embarrassment as well as damage to reputation or relationships. Furthermore, email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.</p> <p>The likelihood of harm is decreased because the breach did not result from malicious intent, but rather human error and the unintended recipients agreed to destroy the information. However, the risk is increased given the nature of the information at issue, the number of unauthorized recipients, and the potential for personal or professional relationships between the unauthorized recipients and the affected individuals.</p> <p>I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization notified affected individuals by email on March 16 and 17 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner