Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	[redacted*], Registered Psychologist, Alberta (Organization)
Decision number (file number)	P2017-ND-106 (File #006154)
Date notice received by OIPC	July 31, 2017
Date Organization last provided information	August 2, 2017
Date of decision	August 2, 2017
Summary of decision	There is a real risk of significant harm to individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident involved the following information as contained in such documents as session case notes, letters, summaries of telephone calls, receipts, invoices, forms, client contact lists, treatment summaries, assessment reports, etc.: • Administrative information: claim numbers, activity numbers, fees for services, payment method (no account number or credit information), session dates, referral source, client's educational institution; • Contact information: first and last names, initials, telephone number, email address; • Personal health information: reason for referral for psychological services, fact of attending psychotherapy, psychological reports, counselling videos, clinical interviews, counselling progress notes, treatment summaries, assessment results, personality questionnaire results, psychological background information, clinical diagnosis, course papers that summarize the case, research audio interviews, audio transcripts, pictures drawn by research participants.

*Publishing the name of the Organization would defeat the intent of the Decision itself to allow the Organization to make an assessment about notification on a case-by-case basis, bearing in mind each individual's particular circumstances and exercising professional judgment.

	In some documents, the information is associated with first and/or last names. However, in other documents, the information is associated with "fake" names or initials only. To the extent the information is about identifiable individuals – either by association with a name or through contextual information – it qualifies as "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 15, 2017, the Organization received an email from Dropbox referencing an access to a Dropbox account from Singapore, but noting that the location may be inaccurate because it was estimated using the IP Address recorded by Dropbox. • The Dropbox account contained certain personal information of former and present clients of the Organization, as well as clients and research participants of other organizations or clinics. • The Organization was unable to obtain additional details of the login from Dropbox (i.e., if files/documents were downloaded, accessed, viewed), despite repeated attempts to do so. • The majority (but not all) of the information at issue was password-protected.
Affected individuals	This incident affected approximately 372 individuals, including 20 former and present clients of the Organization, as well as clients and research participants of other organizations or clinics.
Steps taken to reduce risk of harm to individuals	• Changed the Dropbox password, added another layer of the two-step verification password, and transferred all client-related files and documents to encrypted offline storage. • Identified and protected with a password those files and documents that were not previously password-protected. • Conducted an extensive review of the files and documents stored on the Dropbox account in order to identify the personal information in issue and the affected parties. • Notified the College of Alberta Psychologists.
Steps taken to notify individuals of the incident	Affected individuals have not been notified. The Organization "seeks the Commissioner's assessment as to determine if there is a real risk of significant harm and direct as to whether clients should be notified and by whom."

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
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.	The Organization reported "… if the information were to be accessed and misused, the type of harm that could result could potentially include humiliation and damage to reputation or relationship, and possibly professional opportunities." Further, "Since no financial information is involved, the risk of fraud or identity theft is low, although the risk that the information could be used for criminal purposes cannot be excluded." I agree with the Organization's assessment. Contact, health and profile information (such as lifestyle details, the fact individuals were receiving psychological counselling) could be used to cause the harms of hurt, humiliation, embarrassment and damage to reputation or relationships. Email addresses, particularly in combination with other information, could be used for phishing purposes. These are significant harms.
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.	In assessing the likelihood of harm, the Organization reported: • "We estimate the likelihood of harm occurring as low to medium, given that we have no indication that [the] Dropbox account was targeted and that Dropbox itself stated that the purported location of the login (Singapore) could be inaccurate… The information was exposed for a short period of time only (10 days)… While it is unknown who obtained or could have obtained the information, there is no evidence of malicious intent or purpose." • "… we have no information that access to the personal information by a third party actually took place. The email that was linked to the Dropbox account as well as … other professional and personal email accounts were not compromised nor were there any known unauthorized login/access." • "…we have no indication…that personal information stored in the account has been accessed or used for any unauthorized purpose." • "…clients have a history and current vulnerability of psychological stress related to [a variety of issues]. In my view, there is a real risk of significant harm resulting from this incident. Although the Organization reported there is "no evidence of malicious intent" and "no information that access to the personal information by a third party actually took place", the Organization nonetheless received a notice from Dropbox that a login to the account was detected; if there was such a login, it was an unauthorized, deliberate intrusion.

	Despite some information being password-protected, none of it was encrypted. Although the Organization took steps to mitigate harm (changed passwords, moved information to encrypted offline storage), this was 10 days after the original Dropbox notification of the unauthorized login. The Organization has been unable to obtain additional information from Dropbox to confirm whether or not files/documents were downloaded, accessed or viewed, and it may be that the information continues to be exposed. The Organization can only speculate that the account was not specifically targeted. Finally, based on the Organization's report, it appears that some of the affected individuals may be members of a vulnerable population.

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 who can be identified from the information at issue.

Contact, health and profile information (such as lifestyle details, the fact individuals were receiving psychological counselling) could be used to cause the harms of hurt, humiliation, embarrassment and damage to reputation or relationships. Email addresses, particularly in combination with other information, could be used for phishing purposes. These are significant harms.

Although the Organization reported there is "no evidence of malicious intent" and "no information that access to the personal information by a third party actually took place", the Organization nonetheless received a notice from Dropbox that a login to the account was detected; if there was such a login, it was an unauthorized, deliberate intrusion.

Despite some information being password-protected, none of it was encrypted. Although the Organization took steps to mitigate harm (changed passwords, moved information to encrypted offline storage), this was 10 days after the original Dropbox notification of the unauthorized login. The Organization has been unable to obtain additional information from Dropbox to confirm whether or not files/documents were downloaded, accessed or viewed, and it may be that the information continues to be exposed.

The Organization can only speculate that the account was not specifically targeted. Finally, based on the Organization's report, it appears that some of the affected individuals may be members of a vulnerable population.

I require the Organization to notify the affected individuals who can be identified from the information at issue, and whose personal information is under the Organization's control, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I acknowledge that, in its report to me of this incident, the Organization said that its "…clients have a history and current vulnerability of psychological stress related to [a variety of issues]. As a result, notifying these clients has a high likelihood of causing unnecessary distress and potential harm if the Commissioner deems notification is not required."

I believe the Organization intended to say that "…notifying these clients has a high likelihood of causing unnecessary distress and potential harm if the Commissioner deems notification *is* required." [my emphasis]

I accept that it is possible that, for some clients, notifying them of this incident could cause more harm than the incident itself. However, I require the Organization to make this assessment on a case by case basis, bearing in mind each individual's particular circumstances and exercising professional judgment, and considering various forms of direct notification that may help to offset potential harm, such as meeting with individuals in person or providing verbal notification (rather than sending a letter, for example) so that assistance and support can be immediately provided, and in order to answer any questions that may arise.

In addition, the Organization also reported that "Some of the information in issue belongs to clients of other organizations or individuals whom [the Organization] is currently working with and was working [sic] at a given time including a clinic at an educational institution, two private practices, clinic [sic] at a government organization, and an Employee Assisted Program organization. There are also research participants [sic] information in issue that … were part of [the Organization's] graduate program from courses and thesis research process."

The Organization said that it "seeks the Commissioner's assessment as to determine if there is a real risk of significant harm and direct as to whether clients should be notified *and by whom*." [my emphasis]

The requirement in section 34.1 of PIPA to report incidents to me applies to "An organization having personal information under its control….". Therefore, this breach notification decision applies only to the Organization in respect of personal information (about identifiable individuals) in its control. To the extent this incident involves personal information in the control of other organizations, or public bodies or custodians that may be subject to Alberta's privacy laws other than PIPA, I strongly recommend the Organization notify those other entities about this incident, and provide them with a copy of this breach notification decision as they themselves may have obligations to report this incident and notify affected individuals.

I require the Organization to comply with this breach notification decision within 10 days of the date of the decision, and confirm to me in writing that it has done so.

Jill Clayton
Information and Privacy Commissioner