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	Now in Colour Psychological Services Inc. (Organization)
Decision number (file number)	P2018-ND-111 (File #009392)
Date notice received by OIPC	August 3, 2018
Date Organization last provided information	August 3, 2018
Date of decision	August 13, 2018
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual whose information was collected in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization provides psychological services on behalf of insurance companies and operates in Alberta. The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue includes: • first name and first initial of last name, • names of employees and service providers the client worked with, • titles and dates of previous assessments, • recommendations, • date of psychological session, • clinical information related to return to work progression. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On May 4, 2018, the Organization sent an email to an insurance company's general email address with the intent of submitting an invoice for a client.

	• On July 31, 2018, the Organization discovered that the document attached to the email was about another client. • The incident was discovered when an employee of the insurance company investigated the Organization's request for information about payment of an invoice. The situation became more complex when the insurance company employee copied the information at issue to another insurance company employee who was working with a different client. • The first email (on May 4, 2018) was not encrypted. The second email was password protected and may have been encrypted.
Affected individuals	The incident affected one (1) individual.
Steps taken to reduce risk of harm to individuals	• Reviewed what information was disclosed, how it was disclosed and to whom. • Reviewed electronic communication procedures. Review process is continuing and appropriate changes will be implemented. • Consulted with business partner and Psychologists' Association of Alberta Practice Advisor regarding plan to address breach. • Asked insurance company employees to delete emails and attachments, as per disclaimer statement on initial email.
Steps taken to notify individuals of the incident	The Organization said it has a "Plan to notify client in next session (booked for next week), will offer free counselling to address emotional harm. Will provide referral information to other service providers, if necessary."
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 that "The client may experience negative emotions such as violation and/or shame. Therapeutic rapport may be damaged and this may detract from future engagement with myself and/or other treatment providers." With respect to the sensitivity of the information at issue, the Organization assessed it as: *Low (within insurance company) to moderate (if outside insurance company) – the client provided written consent for her health information to be shared with certain employees of the insurance company using electronic communication; the client's full name was not disclosed, nor was other information that could lead to identity theft; the clinical information disclosed was minimal and vague.* In my view, a reasonable person would consider that the information at issue could be used to cause the harms of hurt, humiliation and embarrassment if disclosed to unauthorized

	recipients outside of the insurance company, or to individuals with whom the affected individual has a personal or professional relationship.
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.	The Organization reported that it considered a number of factors in assessing the likelihood of harm resulting in this case, including: *Who: employees of the insurance company; anyone who can hack an email account.* *Security: lacking when the error was made; encryption of email when error was brought to my attention.* *Sensitivity: low within insurance company; moderate in general cyberspace* *Length of exposure: not sure how to evaluate.* *No evidence of intent to harm.* *Information disclosed is unlikely to be relevant for criminal purposes.* *Information has been recovered and I have requested insurance company employees to delete relevant emails and attachments….* *My client has vulnerabilities but this situation is within her capacity to understand and address.* In my view, the likelihood of harm resulting from this breach is reduced because the incident was the result of human error and not malicious intent. The information was disclosed to a known recipient. However, the Organization seems uncertain as to whom exactly the information may have been disclosed to ("moderate [sensitivity if disclosed] in general cyberspace") and did not report receiving confirmation that the unintended recipients would not use or further disclose the information, or that the information was deleted by the unintended recipient. Instead, the Organization appears to be relying on the disclaimer that was part of the original email ("Asked insurance company employees to delete emails and attachments, as per disclaimer statement on initial email"). I am also concerned due to the length of time that elapsed between the time of the breach and its discovery (almost 3 months).

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 individual.

A reasonable person would consider that the information at issue could be used to cause the harms of hurt, humiliation and embarrassment if disclosed to unauthorized recipients outside of the insurance company, or to individuals with whom the affected individual has a personal or professional relationship. The likelihood of harm resulting from this breach is reduced because the incident was the result of human error and not malicious intent and the information was disclosed to a known recipient.

However, the Organization seems uncertain as to whom exactly the information may have been disclosed to ("moderate [sensitivity if disclosed] in general cyberspace") and did not report receiving confirmation that the unintended recipients would not use or further disclose the information, or that the information was deleted by the unintended recipient. Instead, the Organization appears to be relying on the disclaimer that was part of the original email ("Asked insurance company employees to delete emails and attachments, as per disclaimer statement on initial email"). I am also concerned due to the length of time that elapsed between the time of the breach and its discovery (almost 3 months).

I require the Organization to notify the affected individual whose information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and **confirm to my office in writing within 10 days of the date of this decision that it has done so.**

Jill Clayton
Information and Privacy Commissioner