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	Tina Cowan, Counseling Services, Registered Provisional Psychologist, Alberta (Organization)
Decision number (file number)	P2019-ND-146 (File #007310)
Date notice received by OIPC	December 8, 2017
Date Organization last provided information	February 24, 2018
Date of decision	August 19, 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 the 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in the incident: • name, • address, • telephone number, • email, • date of birth, • prior counselor, • hourly rate for session, • handwritten counseling notes, • activity or exercise sheets completed by clients during counseling sessions, • supervising notes (discussions between provisional psychologist and supervising psychologist) regarding patient progress and suggestions for topics to address and different therapeutic techniques, • client emails describing the nature of issues and correspondence related to scheduling.

	This information is about identifiable individuals 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 November 29, 2017, the Organization found that a briefcase and cellphone had been stolen from a shared office space. • The stolen briefcase contained 5 paper-based client files (for 8 individuals), a binder containing paper-based supervision notes (for 53 individuals), and a paper-based notebook that contained contact information and hourly rate session fee (for 74 clients). • The cell phone did not have any access controls.
Affected individuals	The incident affected seventy-four (74) individuals.
Steps taken to reduce risk of harm to individuals	• Offered counseling to affected individuals. • Installed a security camera. • Reported incident to law enforcement, as well as professional and privacy regulators.
Steps taken to notify individuals of the incident	All affected individuals were notified either by email, telephone or in person. Notifications occurred between January 10 and February 23, 2018.
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 primary types of harm that may result from the breach are humiliation, damage to reputation, and damage to relationships associated with the disclosure of sensitive information regarding mental health and other personal issues such as marital or relationship issues". I agree with the Organization's assessment. A reasonable person would consider that the medical/health information at issue could be used to cause the harms of hurt, humiliation and embarrassment as well as damage to reputation or relationships. Identity information (date of birth), particularly in conjunction with other information, could be used for identity theft and fraud purposes. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.

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 resulting from this incident, the Organization reported: • "It is not possible to ascertain who obtained or could have obtained access to the information. Any individual who physically removed the items from the premises would have access to the contents of the briefcase and the cellular telephone, as described. There is no indication that the theft was motivated by anything other than an attempt to find money or valuables." • "The perpetrator would have had access to the information from the time that the theft occurred, and will continue to have access to paper records. Any continued electronic access to the gmail account would no longer have been possible as of November 2, 2017, 8:48pm." • "There is no evidence that the perpetrator was specifically targeting the information". • "...the most sensitive information (the client file notes and supervisions notes) were handwritten…and may be difficult for third parties to read." • "The information has not been recoved [sic]." • "There are some vulnerable clients involved." • "[The Organization] has no indication that the perpetrator has used or intends to use any of the information to harm the affected clients." In my view, a reasonable person would consider the likelihood of harm is increased as the incident resulted from malicious intent (theft) and the information has not been recovered. Information stored on the cell phone was accessible for almost 5 hours. The affected individuals are part of a vulnerable population. The lack of reported incidents to date does not mitigate against future harmful use of the information. The Organization can only speculate as to the motives of the perpetrator.
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 medical/health information at issue could be used to cause the harms of hurt, humiliation and embarrassment as well as damage to reputation or relationships. Identity information (date of birth), particularly in conjunction with other information, could be used for identity theft and fraud purposes. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.	

The likelihood of harm is increased as the incident resulted from malicious intent (theft) and the information has not been recovered. Information stored on the cell phone was accessible for almost 5 hours. The affected individuals are part of a vulnerable population. The lack of reported incidents to date does not mitigate against future harmful use of the information. The Organization can only speculate as to the motives of the perpetrator.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand all affected individuals were notified either by email, telephone or in person between January 10 and February 23, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner