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	Vecova Centre for Disability Services and Research (Organization)
Decision number (file number)	P2019-ND-132 (File #012176)
Date notice received by OIPC	February 26, 2019
Date Organization last provided information	February 26, 2019
Date of decision	August 12, 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 incorporated under Alberta's *Societies Act* and is a "non-profit organization" as defined in section 56(1)(b)(i) of PIPA. Under sections 56(2) and (3), PIPA only applies to personal information that is collected, used or disclosed by non-profit organizations in connection with a commercial activity. Pursuant to section 56(1)(a) of PIPA, a "commercial activity" is any transaction, act, conduct, or regular course of conduct that is of a commercial character. The Organization reported that it "…provides an Empower Abilities Program…for children and youth with mild to moderate motor delays and disabilities… [and] charges a fee for the services provided under the Program, which is paid by the Participant's parent/guardian(s)." This is a commercial activity such that PIPA applies in this matter.
Section 1(1)(k) of PIPA "personal information"	The following personal information of three participants in the program was contained in Participant files: • name, • date of birth, • phone number, • parent/guardian email address,

	• parent/guardian(s)' name, • diagnosis, • history, • extra-curricular activities, • presenting concerns, • gross motor functioning, • standardized assessment, and • overall impression and recommendations. In addition, the following personal information of an additional 85 participants and/or their parents or guardian was stored in Server Files: • name, • date of birth, • phone number, • parent/guardian(s)' name, • email address. This information is about identifiable individuals is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 12, 2019, between approximately 11:30 a.m. - 12:00 p.m., a laptop used by a physiotherapist was stolen from an office accessed through a classroom within the Organization's Calgary premises. • The laptop contained the files for three program participants. The files were stored on the desktop of the laptop which was not encrypted. • The laptop also contained information on an encrypted server/drive relating to an additional 85 participants and their parents/guardians. • The incident was discovered within 30 minutes of its occurrence and the laptop's log-in credentials were changed remotely, restricting access to the server files which were immediately encrypted. The Organization estimates that the maximum amount of time the laptop could have been in the possession of the third party before the log-in credentials were remotely changed was one hour. • The laptop has not been recovered.

Affected individuals	The incident affected the following individuals: • Participant files: 3 minors, 3 adults • Server files: 85 minors, 118 adults
Steps taken to reduce risk of harm to individuals	• Investigated and remotely changed the access credentials for the laptop. • Offered identity theft monitoring to the parents of all affected individuals for 1 year at no cost, and fraud monitoring to all affected minor individuals for 6 years at no cost. • Will continue to educate and train employees regarding the importance of compliance with policies relating to safety and security of workspaces. • Reviewing physical and technical security measures and procedures.
Steps taken to notify individuals of the incident	All affected individuals were sent written notification of the incident on February 26, 2019.
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 "…the disclosure of the Participant Files and Server Files could potentially cause affected individuals to suffer from the harms of humiliation/embarrassment, damage to reputation as well as identity theft/fraud (including a risk of phishing attacks)." In my view, a reasonable person would consider the contact, identity and health/medical information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing increase vulnerability to identity theft and fraud. 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.	The Organization reported: *The likelihood that harm may occur to affected individuals as it relates to the Participant Files is moderate. The Participant files would have been immediately accessible if the third party was able to bypass the password protection for the laptop and the sensitivity of the personal information contained within the Participant Files is high.* *The likelihood that harm may occur to affected individuals regarding the Server Files is low to moderate.* *The theft of the laptop was immediately discovered and credentials to the laptop remotely changed shortly thereafter. The third party would have had a limited amount*

	of time (maximum 1 hour) to bypass the password protection on the laptop before log-in credentials were remotely changed… and access restricted. Additionally, in the event the password was entered three times incorrectly, the laptop would become locked, further restricting access. *While [the Organization] is not aware of any personal information of any affected individual being mis-used, it has not recovered the laptop and cannot determine if the Server Files were accessed by a third party at any point in time. Additionally the Incident was caused as a result of the theft of the laptop (malicious intent) rather than a mistake, which increases the likelihood that harm could result to affected individuals.* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (theft). The information has not been recovered. I agree with the Organization that the likelihood of harm with respect to the Server Files is lower; however, the laptop has not been recovered and the Organization "cannot determine if the Server Files were accessed by a third party at any point in time."

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 in this case.

A reasonable person would consider the contact, identity and health/medical information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing increase vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (theft). The information has not been recovered. I agree with the Organization that the likelihood of harm with respect to the Server Files is lower; however, the laptop has not been recovered and the Organization "cannot determine if the Server Files were accessed by a third party at any point in time."

The Organization is required to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified all affected individuals were sent written notification of the incident on February 26, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner