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	CDSPI (Organization)
Decision number (file number)	P2021-ND-079 (File #012917)
Date notice received by OIPC	April 2, 2019
Date Organization last provided information	April 2, 2019
Date of decision	March 9, 2021
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 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 incident involved all or some of the following information: • name, • address, • email address, • telephone number, • date of birth, • account number with Organization, • university, and • medical history. 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 March 12, 2019, an employee with the Organization inadvertently enclosed a copy of an individual's application for insurance in a letter to another client of the Organization. • On March 20, 2019, the unintended recipient telephoned the Organization to report the error.
Affected individuals	The incident affected 1 individual.
Steps taken to reduce risk of harm to individuals	• Confirmed that the unintended recipient destroyed the information without copying it or disclosing it to anyone else. • Reiterated with the administrative staff the importance of privacy and ensuring all documents being sent to clients are for the intended recipient. • Implemented another check point into the process whereby a second person will review documents being mailed out that contain medical data, to ensure all documents belong to the intended recipient.
Steps taken to notify individuals of the incident	The affected individual was notified by telephone call on March 29, 2019 followed by a letter sent on April 2, 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 that "The breach could result in fraud, identity theft, hurt, humiliation, and embarrassment to the affected individual." I agree with the Organization's assessment. A reasonable person would consider the contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses (particularly in conjunction with other information) could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation, and embarrassment. These are all 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 that "The incident resulted from human error rather than malicious intent and the unintended recipient reported the breach to the Organization and confirmed that she destroyed the information and did not disclose the information to any person. However, there could be a professional connection between the affected individuals and the unintended recipient as both are enrolled in university programs to become members of the same profession, even though those university programs are located in different provinces." 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. However, while I agree it is unlikely that the unauthorized recipient would use the information for identity theft, fraud or phishing purposes, the possible professional connection increases the likelihood of hurt, humiliation or embarrassment resulting from the breach.

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 the contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses (particularly in conjunction with other information) could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation, and embarrassment. These are all significant harms.

The likelihood of harm is decreased because the breach did not result from malicious intent, but rather human error. However, while I agree it is unlikely that the unauthorized recipient would use the information for identity theft, fraud or phishing purposes, the possible professional connection increases the likelihood of hurt, humiliation or embarrassment resulting from the breach.

I require the Organization to notify the affected individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual by telephone call on March 29, 2019 followed by a letter sent on April 2, 2019, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner