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	Ascensia Diabetes Care Holdings AG (Organization)
Decision number (file number)	P2019-ND-089 (File #010213)
Date notice received by OIPC	October 30, 2018
Date Organization last provided information	February 7, 2019
Date of decision	June 26, 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 those individuals whose personal 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 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, • blood glucose level, and • hashed password. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's application for mobile devices.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization provides and operates an application for mobile devices to measure blood glucose level through a connected blood glucose meter.

	• The application synchronizes data with the Organization's servers in the cloud to allow customers to use their data with further mobile devices which are also synchronized with the servers. • The Organization reported that "Penetration testing conducted on 16 October 2018 revealed a vulnerability as a consequence of which we cannot exclude that third parties could have gained access to personal data".
Affected individuals	The total number of affected individuals is 52,103. Based on the information available, there were 1,651 Alberta residents affected by the breach.
Steps taken to reduce risk of harm to individuals	• Identified the vulnerability. • Immediately and permanently fixed the root cause of the security vulnerability. • Analyzed server logs for 30 days and the logs showed no sign of exploitation of the vulnerability.
Steps taken to notify individuals of the incident	Affected individuals were notified by email between December 6 and December 12, 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 did not specifically identify any harm that might result from this incident. In my view, a reasonable person would consider that the contact information (and particularly email address) could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Medical/health information could be used to cause 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 did not specifically provide an assessment of the likelihood that significant harm would result from this incident but did report that it "…analyzed our server logs for the last 30 days and the logs did not show any sign of exploitation of this vulnerability. Also, we consider it highly unlikely that any user data has been accessed prior to these 30 days period covered by the log files as exploiting the vulnerability would have required professional programming skills." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is reduced because the breach does not appear to be the result of malicious intent (no deliberate action). However, the Organization did not report how long the information may have been exposed or why it only reviewed 30 days

	of server logs. The Organization reported that it could not exclude that third parties could have gained access to personal data. Phishing/identity theft and fraud can occur months and even years after a data 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 individuals.

A reasonable person would consider that the contact information (and particularly email address) could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Medical/health information could be used to cause hurt, humiliation and embarrassment. These are all significant harms. The likelihood of harm resulting from this incident is reduced because the breach does not appear to be the result of malicious intent (no deliberate action). However, the Organization did not report how long the information may have been exposed or why it only reviewed 30 days of server logs. The Organization reported that it could not exclude that third parties could have gained access to personal data. Phishing/identity theft and fraud can occur months and even years after a data breach.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email between December 6 and December 12, 2018, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner