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	Kalispell Regional Healthcare (Organization)
Decision number (file number)	P2020-ND-128 (File #013758)
Date notice received by OIPC	October 23, 2019
Date Organization last provided information	October 23, 2019
Date of decision	October 30, 2020
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 located in Kalispell, Montana, USA. The Organization says it "…does not accept that the privacy breach reporting provisions of the Personal Information Protection Act, 2003 C. P-6.5 are applicable in this matter", but does not explain why that is the case. In my view, the Organization is an "organization" as defined in section 1(1)(i) of PIPA, and to which PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • medical record number, • date of birth, • telephone number, • email address, • medical history and treatment information, • date of service, • treating/referring physician, • medical bill account number and/or health insurance information.

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In the summer of 2019, the Organization discovered that several employees were victims of an email that led them to unknowingly provide their login credentials to malicious criminals. • On August 28, 2019, the Organization learned that some patients' personal information may have been accessed without authorization. A deeper investigation determined that some personal information may have been accessed as early as May 24, 2019.
Affected individuals	The Organization assesses there may be approximately 475 Albertans for whom there may be a real risk of harm.
Steps taken to reduce risk of harm to individuals	• Disabled accounts. • Notified US federal law enforcement. • Launched an investigation, which was performed by a nationally-recognized digital forensics firm. • Reviewed security measures in an effort to prevent a similar incident from occurring. • Provided fraud consultation services to the individuals free of charge
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on October 22, 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 did not specifically identify possible harm(s) that might result from the incident, but reported that it "…provided fraud consultation services" to affected individuals. In my view, a reasonable person would consider that the contact, identity, and medical information at issue could be used to cause the harms of identity theft and fraud. Medical information could also be used to cause the harms of embarrassment and humiliation. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Login credentials could be used to compromise other online accounts. 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 assess the likelihood of harm resulting from this incident. In my view, the likelihood of harm resulting from this incident is increased because it appears to be the result of malicious intent (deliberate intrusion) and information may have been exposed over a period of weeks or 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 individuals.

A reasonable person would consider that the contact, identity, and medical information at issue could be used to cause the harms of identity theft and fraud. Medical information could also be used to cause the harms of embarrassment and humiliation. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Login credentials could be used to compromise other online accounts. These are all significant harms.

The likelihood of harm resulting from this incident is increased because it appears to be the result of malicious intent (deliberate intrusion) and information may have been exposed over a period of weeks or months.

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 affected individuals were notified by mail on October 22, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner