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	EPCOR Energy Alberta LP (Organization)
Decision number (file number)	P2023-ND-009 (File #027674)
Date notice received by OIPC	October 7, 2022
Date Organization last provided information	January 27, 2023
Date of decision	February 2, 2023
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: • personal email address, • a message from affected individual to Organization re: Short Term Disability, which referenced a doctor's note, • email response from the sender indicating that the affected individual is on an unpaid leave of absence and resulting impacts on employee benefits, • detailed information from the sender regarding mental health supports available to employees. This information is about identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies. The Organization reported that the details of the claim and details of the affected individual's treatment were not included in the misdirected email.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• On September 22, 2022, an employee misdirected an email containing personal information about the affected individual who is also an employee. • The unintended recipient, who is also an employee, alerted the Organization of the mistake.
Affected individuals	The incident affected one (1) individual.
Steps taken to reduce risk of harm to individuals	• Initiated an internal privacy investigation. • Obtained a commitment from the unintended recipient that they would keep the contents of the misdirected email confidential. • Received written confirmation that the unintended recipient permanently deleted the information. • Spoke with the unintended recipient in order to ensure the unintended recipient understood the meaning of confidentiality and discuss potential consequences of failing to keep the contents of the misdirected email confidential. • Will offer the affected individual access to a mental health professional at the Organization's cost to ensure they have the option of discussing this matter with a trained professional following notification.
Steps taken to notify individuals of the incident	The Organization reported that it "*will notify the affected individual in due course."* Recently, the Organization reported it intends to schedule a virtual meeting to provide notification in the coming weeks. It also intends to provide written notice.
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 possible harms that may occur as a result of the breach are: *Reputational harm, embarassment (sic), humiliation, hurt, anxiety, stress.* I agree with the Organization's assessment. A reasonable person would consider that the contact and medical information at issue could be used to cause reputational harm, hurt, humiliation, embarrassment, anxiety and stress embarrassment. These are all significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation	The Organization reported, *...At this time, we believe that the risk is low that the unintended recipient will cause any further harms of*

or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	*embarrassment (sic), humiliation, hurt, anxiety, stress, as it is expected that the unintended recipient will keep the contents of the misdirected information confidential. To date, the unintended recipient has been highly cooperative and (a) is an existing employee (b) immediately contacted the sender to report the incident (c) has committed to keeping the contents of the misdirected email confidential and to cooperatiing (sic) with EPCOR in remediating the issue (d) has permanently deleted the misdirected email.* When asked for further information concerning the size and structure of the workplace, the Organization reported, *Due to the timing of their hiring, the option of working from home, and respective leaves, we believe that the affected individual and unintended recipient have likely not worked together in the same physical space which explains why the unintended recipient has stated that they do not know the affected individual. These individuals are part of the same "work group".* The Organization reported the work group is comprised of a small number of people who perform similar job functions under one manager. In my view, a reasonable person would consider the likelihood of harm resulting from this incident is decreased because the breach is the result of human error and not malicious intent. However, although the Organization put safeguards in place to prevent further embarrassment, reputational harm, and stress, the affected individual and the unintended recipient have a professional connection in a small workplace. While they may not work together in the same space due to alternative work arrangements , the affected individual and the unintended recipient both work in the same area of the organization and report to the same supervisor, which increases the likelihood of harm to the affected individual.

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.

The contact and medical information at issue could be used to cause reputational harm, hurt, humiliation, embarrassment, anxiety and stress embarrassment. These are all significant harms.

The likelihood of harm resulting from this incident is decreased because the breach is the result of human error and not malicious intent. However, although the Organization put safeguards in place to prevent further embarrassment, reputational harm, and stress, the affected individual and the

unintended recipient have a professional connection in a small workplace. While they may not work together in the same space due to alternative work arrangements, the affected individual and the unintended recipient share a small work group and report to the same supervisor, which increases the likelihood of harm to the affected individual.

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

The Organization reported *"in order to prioritize the affected individual's mental health and general well-being, a decision was made to temporarily delay notification."*." The Organization stated in recent correspondence that it intends to notify the affected individual soon in a virtual meeting. It also intends to provide written notice.

Section 37.1(2) of PIPA states "… the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate…"

Bearing in mind the concern expressed by the Organization about prioritizing the health of the affected individual, I require the Organization to make an assessment of the harm that may be caused by providing notice and to exercise professional judgement in providing the notice. It may consider seeking a professional opinion about the timing and manner of the notification from a health service provider. It may consider various forms of direct notification, such as an in person meeting so that assistance and support can be immediately provided. Perhaps that result may be achieved virtually as well.

The notification must be in accordance with section 19.1 of the *Personal Information Protection Regulation*. The Organization is also required to inform my Office, within ten (10) days of the date of this decision, when the affected individual is to be notified of this incident.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner