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	National Capital Poison Center (Organization)
Decision number (file number)	P2019-ND-152 (File #007382)
Date notice received by OIPC	December 19, 2017
Date Organization last provided information	January 5, 2018
Date of decision	August 21, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is based in Washington, D.C., USA and 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 of caller, • name of person exposed to poisonous substance, • date of birth, • address, • telephone number, • information about exposure, • clinical course, • recommendations provided to the caller, • caller's email address, and • treating facility name and medical record number, if applicable. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from individuals who telephoned the Organization. To the extent the personal information was collected in Alberta, PIPA applies in this matter.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On October 21, 2017, the Organization discovered it had experienced a ransomware infection. • The Organization's investigation determined that unauthorized access to a database server occurred on October 21, 2017, and unauthorized access to the data stored on that server cannot be ruled out. • The possibly affected database contains information that may have been provided during the Organization's call centre calls.
Affected individuals	The incident affected 43 individuals with Alberta area codes; however, the Organization is unable to determine if these 43 calls were from, or related to, Alberta residents.
Steps taken to reduce risk of harm to individuals	• Investigated and retained a third-party forensic investigator. • Restored all data and functionality from backups and regained access to its information. • Notified other state and foreign regulators and the major consumer reporting agencies, as necessary. • Enhanced the security of its systems. • Continues to monitor its environment for suspicious activity. • Notified potentially impacted individuals.
Steps taken to notify individuals of the incident	The Organization reported it "…has insufficient contact information for those individuals residing in Alberta that may be impacted by this incident, and the total number of potentially impacted residents is unknown". However, the Organization provided substitute notice to potentially impacted individuals by way of a notice on its website homepage (www.poison.org), as well as publishing notices to certain state media outlets and publications. The Organization also established a dedicated assistance line for individuals seeking additional information regarding the incident.
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, but its news release said "While the types of information that are potentially compromised as a result of this incident are not those that can be easily used to perpetrate identity theft, fraud, harm, or loss, and [the Organization] has received no reports of actual or attempted misuse of the information involved in this incident, [the Organization] encourages everyone to remain vigilant against incidents of identity theft …".

	In my view, a reasonable person would consider the contact and identity information (date of birth) 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/health 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 did not specifically assess the likelihood that significant harm would result from this incident but did report that it "… has received no reports of attempted or actual misuse of this information". In my view, a reasonable person would consider 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 (deliberate intrusion and ransomware). The Organization was able to restore data and functionality from backups; however, the Organization is unable to rule out unauthorized access to the data stored on the server.

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 the contact and identity information (date of birth) 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/health information could be used to cause the harms of hurt, humiliation, and embarrassment. These are all 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 (deliberate intrusion and ransomware). The Organization was able to restore data and functionality from backups; however, the Organization is unable to rule out unauthorized access to the data stored on the server.

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). Section 19.1(1) of the Regulation states that the notification must "… be given directly to the individual…" , although section 19.1(2) says "… the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

In this case, the Organization reported that direct notification would not be possible because it "…has insufficient contact information for those individuals residing in Alberta that may be impacted by this incident, and the total number of potentially impacted residents is unknown". However, the Organization provided substitute notice to potentially impacted individuals by way of a notice on its website homepage (www.poison.org), as well as publishing notices to certain state media outlets and publications. The Organization also established a dedicated assistance line for individuals seeking additional information regarding the incident.

Given the Organization's submissions, I accept that indirect or substitute notice as described by the Organization is reasonable in this case, where the Organization is unable to contact affected individuals directly.

Jill Clayton
Information and Privacy Commissioner