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	Alberta Medical Association (Organization)
Decision number (file number)	P2019-ND-094 (File #011997)
Date notice received by OIPC	February 11, 2019
Date Organization last provided information	February 11, 2019
Date of decision	June 27, 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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization reported that it is incorporated under Alberta's *Societies Act* and therefore is a "non-profit organization" as defined in section 56(1)(b)(i) of PIPA. Pursuant to section 56(2), PIPA "does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization", except in the case of personal information that is collected, used or disclosed in connection with any commercial activity. It appears that the personal information involved in this incident was collected, used and disclosed by the Organization for the purposes of providing insurance services to its members. In my view these services are a "commercial activity" in that they are similar to that of any insurance business operated in the private sector, including that members pay a competitive rate for the insurance they receive. Accordingly, PIPA applies in this matter.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • name of family member receiving benefits, • professional corporation name and number,

	• member number, • benefit cheque addressed and included with statement, • generic description of medical expenses e.g., vision, Rx, etc. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• Between February 4, 2019 and February 8, 2019, an employee was processing benefit cheques and corresponding benefit statements. Due to a duplexing error, some clients inadvertently received their own statement, as well as information related to another client. • The incident was discovered on February 7, 2019, when a client emailed the Organization informing it of the error and requesting a new statement be issued. On February 8, 2019, another client left a voicemail message reporting receiving someone else's information.
Affected individuals	The incident affected 8 individuals.
Steps taken to reduce risk of harm to individuals	• Examined statements in the shredding console to determine the potential number of clients that could be affected by the breach. • Making arrangements to require clients to access claim statements online. • Implementing a more stringent authentication process when staff speak to members on the phone, or accept e-mail instructions from them.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on February 8, 2019 and February 9, 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 the possible harms that might result from this incident include: *Possible embarrassment for the client who's statement was sent to another client because now the other client will know they deal with the [Organization], the names of their family members, what their cost plus limit is, what total dollar value they submitted, their [Organization] member number as well as their Professional Corporation name and number.* *Due to the amount of information provided on the HBTF*

	statement, the potential does exist for the recipient of someone else's statement to phone in and identify themselves using the information on the statement to try to access another client's information. I accept the Organization's assessment. The contact, medical and benefits information at issue could be used to cause the harms of identity theft and fraud, as well as potentially embarrassment. These are 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 "All HBTF clients are also …members who also are professional members of the CMA and therefore adhere to a professional code of conduct and ethics policy." In my view, a reasonable person would consider that the risk of significant harm is decreased as the breach did not result from malicious intent, but rather a duplexing error. Given that the recipients of the information are all members of the Organization, in my view identity theft and fraud are unlikely. However, this also increases the likelihood of personal/professional relationships between the affected individuals and the recipients of the information, increasing the likelihood of embarrassment. The Organization did not report any efforts to retrieve the information sent in error.

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.

The contact, medical and benefits information at issue could be used to cause the harms of identity theft and fraud, as well as potentially embarrassment. These are significant harms. The risk of significant harm is decreased as the breach did not result from malicious intent, but rather a duplexing error. Given that the recipients of the information are all members of the Organization, in my view identity theft and fraud are unlikely. However, this also increases the likelihood of personal/professional relationships between the affected individuals and the recipients of the information, increasing the likelihood of embarrassment. The Organization did not report any efforts to retrieve the information sent in error.

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

I understand that affected individuals were notified by email on February 8, 2019 and February 9, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner