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	Medical Informatics Engineering and NoMoreClipboard (a wholly owned subsidiary) (collectively, the Organization)
Decision number (file number)	P2016-ND-67 (File #001701)
Date notice received by OIPC	October 14, 2015
Date Organization last provided information	October 23, 2016
Date of decision	December 20, 2016
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 is incorporated in the state of Indiana and operating in Alberta. It is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • mailing address, • username, • hashed password, • security question and answer, • email address, • date of birth, • Social Insurance Number, • lab results, • doctor's name, • insurance policy information, • diagnosis,

	• disability code, • medical conditions, • telephone number, • spousal information (name and date of birth), and • children's information (name, birth weight and size). 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 26, 2015, the Organization discovered suspicious activity in one of its servers. • The Organization's investigation revealed that an unauthorized third party gained access to some individuals' personal information stored on its servers.
Affected individuals	The incident affected 40 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified affected individuals and law enforcement. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta. • Offered free identity theft recovery and credit monitoring services.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on October 2, 2015.
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.	In its report of the incident, the Organization did not specifically identify any harm that might result to affected individuals. However, it did report that it had "established a toll-free hotline to answer questions about this incident and to provide information relating to protection against identity theft and fraud."

	The personal information involved in this incident includes sensitive identity and health information. This information could be used to cause the harms of identity theft and fraud, as well as hurt and humiliation due to the sensitivity of some of the health-related information. These are significant harms. In addition, email addresses and security questions and answers could be used to gain unauthorized access to other accounts and cause the significant harm of phishing.
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 provide its assessment of the risk of harm to affected individuals. In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised as a result of the malicious action (deliberate intent) of an unknown third party and has not been recovered.

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 personal information involved in this incident includes sensitive identity and health information. This information could be used to cause the harms of identity theft and fraud, as well as hurt and humiliation due to the sensitivity of some of the health-related information. These are significant harms. In addition, email addresses and security questions and answers could be used to gain unauthorized access to other accounts and cause the significant harm of phishing. The likelihood of harm resulting from this incident is increased because the personal information was compromised as a result of the malicious action (deliberate intent) of an unknown third party and has not been recovered.

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 the Organization notified the affected individuals in a letter dated October 2, 2015, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner