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	Homewood Health Inc. (Organization)
Decision number (file number)	P2021-ND-284 (File #022574)
Date notice received by OIPC	August 3, 2021
Date Organization last provided information	January 31, 2022
Date of decision	February 22, 2022
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 provides organizational wellness and employee and family assistance programs (EFAP). It is headquartered in Guelph, Ontario, operates in Alberta, 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, • location (city, country), • telephone number, • email address, • emails, • gender, • date of birth, • counselling services provided, • counselling issues, • plan holder / dependent names, • audiences attending counselling, • client status (new or existing), • whether client is an employee, family member, or a dependent, • coaching received, • disability treatment, • wellness session information,

	• line crisis management services, • "goal attainment," • dates of events, • employment position, • employment tenure information, and • employment "safety sensitive" status. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization was the subject of a cyber-attack which resulted in the exfiltration and publication of client personal information on the data marketplace "Marketo." • The Organization's investigation determined that the attack on the network began on or about March 9, 2021, when an unknown device accessed the server(s) and exfiltrated records. • It is believed the threat actor obtained credentials via phishing, then used offensive tools (Cobalt Strike) to propagate the attack. The attacker also attempted to deploy additional malware payloads. • The Organization first received threatening emails from a threat actor in May 2021. These emails were thought to be innocuous; despite this, the Organization engaged its external cybersecurity team for investigation. • On June 11, 2021, the Organization's external security team obtained a sample of the exfiltrated records, and on June 22, 2021, determined that files contained personal information.
Affected individuals	The incident affected approximately 19,677 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified law enforcement agencies. • Engaged cybersecurity experts to assist with incident response. • Removed the records from the internet and obtained assurances that the threat actor destroyed the records and will not disseminate the data further. • Ongoing monitoring of data disclosure sites and the dark web. • Investing in training, including mandatory, audited, online training modules for all employees.

	• Following up with third parties who may have had access to the sample data to ensure personal information has been securely destroyed.
Steps taken to notify individuals of the incident	The Organization reported direct notification "is not possible in this situation" and requested authorization for "indirect notification, which would involve notification through employer organizations" as well as through public notice placed on its website. The Organization provided the following reasons: • *There is limited contact information available. [The Organization] does not collect mailing addresses as part of its EFAP services. The only contact information that it has access to is telephone number or email address. Some of the reports go back a number of years and it is likely that the information is no longer accurate or up to date.* • *There is significant potential for harm associated with direct notification given the nature of the services. EFAP services include mental health and addictions counselling. Receipt of a letter, email or telephone call from [the Organization] may result in the inadvertent disclosure of personal information. Family members/dependents often receive EFAP services without the knowledge of the employee or other family members. There may be situations associated with higher risk as well, for example, custody and access issues and abuse situations.* • *There are a large number of potentially affected individuals, which makes direct notification impractical.* • *If individuals would like more information, their current contact information would be collected along with consent for [the Organization] to follow up with the individual directly. [The Organization] would be able to send notification letters directly through this process.* In later submissions, the Organization advised that affected individuals were notified indirectly, on or about January 31, 2022, by way of notices distributed by employer organizations and a public notice on the Organization's website. The Organization also said that it "will post notice through media".

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 risk of harm is high (reputational, emotional, etc)." Additionally, the Organization said: *Personal information is in the hands of a criminal organization that is hosting stolen personal information on a website for sale. The personal information relates to confidential EFAP sessions and is sensitive in nature.* In my view, a reasonable person would consider that the identity, contact, medical (counselling, treatment, crisis line), and employment information at issue could be used to cause the harms of embarrassment, hurt or humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, and blackmail or extortion. Other harms may occur in "situations associated with higher risk … for example … access issues and abuse situations" as described in the Organization's breach report. Email addresses could be used for the purposes of phishing or spear-phishing, increasing affected individuals' vulnerability to the above, and possibly, the additional harms of identity theft and fraud. Further, the Organization's analysis of affected records is ongoing; it is not clear what other possible harms may exist; nonetheless, the above 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.	Initially, the Organization reported "The risk of harm is high…". The Organization subsequently reported: *At this time, it is believed that risk of possible harm to affected individuals is low as the breach has been contained and information removed from the internet.* *The "sample data" has been removed from the web and is no longer accessible. Further, working closely with experts familiar with cyber-attacks and negotiations with cyber criminals, [the Organization] has received a detailed accounting of the stolen data and has taken steps to validate its secure destruction.* *[The Organization] has engaged cybersecurity experts to perform ongoing Marketo, Clearnet and dark web TOR*

	sites monitoring to ensure that there is no further disclosure of personal information. *[The Organization] is following up with any third parties, including media, who may have had access to the sample data to determine if there was any unauthorized access to or disclosure of personal information. [The Organization] will take any necessary steps to ensure that personal information has been securely destroyed.* *The risk of possible harm to affected individuals continues to be assessed as low for the big data set; the risk of possible harm to affected individuals is higher for those individuals whose personal information was in the Sample Data Pack.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion, attempted deployment of malware, publication of personal information, extortion). Despite removing the "sample data" from the web, the personal information was nonetheless exposed. It is not certain whether copies of the information were created prior to its removal from the internet. It is also unclear whether the threat actor's assurances that records have been destroyed, and will not be disseminated further, are reliable. Additionally, the Organization's report indicates its systems were breached in March 2021, suggesting that records were exposed for approximately five (5) months prior to the date the breach was reported.

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 identity, contact, medical (counselling, treatment, crisis line), and employment information at issue could be used to cause the harms of embarrassment, hurt or humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, and blackmail or extortion.

Other harms may occur in "situations associated with higher risk … for example … access issues and abuse situations" as described in the Organization's breach report.

Email addresses could be used for the purposes of phishing or spear-phishing, increasing affected individuals' vulnerability to the above, and possibly, the additional harms of identity theft and fraud.

Further, the Organization's analysis of affected records is ongoing; it is not clear what other possible harms may exist; nonetheless, the above 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 a third party (deliberate intrusion, attempted deployment of malware, publication of personal information, extortion).

Despite removing the "sample data" from the web, the personal information was nonetheless exposed. It is not certain whether copies of the information were created prior to its removal from the internet. It is also unclear whether the threat actor's assurances that records have been destroyed, and will not be disseminated further, are reliable.

Additionally, the Organization's report indicates its systems were breached in March 2021, suggesting that records were exposed for approximately five (5) months prior to the date the breach was reported.

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…", however 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 provided a submission explaining why direct notice is not possible. Additionally, the Organization submitted a plan for indirect notice, involving the distribution of notifications through employers as well as a public notice on the Organization's website.

Given the Organization's submission, I accept that indirect notice as described by the Organization is reasonable in this case, where the Organization is unable to contact the affected individuals directly. I understand that affected individuals were notified indirectly, on or about January 31, 2022, by way of notices distributed by employer organizations and a public notice on the Organization's website.

Jill Clayton
Information and Privacy Commissioner