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	Pureform Diagnostic Imaging Clinics Inc. (Organization)
Decision number (file number)	P2021-ND-338 (File #020633)
Date notice received by OIPC	April 14, 2021
Date Organization last provided information	October 5, 2021
Date of decision	March 10, 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 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 about current and former employees: • name, • address, • contact information, • tax forms, • RRSP enrolment forms, • employment agreements, • employee evaluations, and • payroll information. The incident involved all or some of the following information about patients: • name, • procedure date, • type of procedure, and • procedure results.

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. I note, however, that the Organization's website says it is "a boutique provider of community based Diagnostic Imaging services … [who] work with over fourteen Radiologists to provide a range of sub-specialties …". Some of the Organization's work "Requires a valid health care card and a referral from a medical doctor, chiropractor, or qualified physiotherapist." Given this, some of the information at issue may qualify as "health information" as defined in Alberta's *Health Information Act* (HIA). Pursuant to section 4(3)(f), PIPA does not apply to "health information as defined in the *Health Information Act* to which that Act applies." Therefore, to the extent the information at issue in this matter is health information as defined in HIA, PIPA does not apply.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 20, 2021, the Organization was subject to a ransomware attack (Sodinokibi). The breach was discovered on the same day when employees noticed they were unable to access information on affected systems; a ransom note was also found. • The Organization reported that the threat actor gained access to the Organization's network via a brute-force attack against an employee user account. The threat actor subsequently uploaded the malicious payload and exfiltrated records.
Affected individuals	The incident affected 208 current and former employees and 931 patients in Alberta.
Steps taken to reduce risk of harm to individuals	• Took all systems offline. • Retained forensic specialists to investigate the incident. • Retained a cybersecurity firm to engage in incident response. • Engaged a cyber insurance company to provide breach management services and guidance. • Engaged specialized firms to enhance information security. • Provided identity theft and credit monitoring services to affected individuals. • Fully audited areas of potential concern.

	• Rebuilt several IT systems including active directory, thereby resetting all user credentials (via creation of new accounts). • Implemented hardware and software deployment recommendations including upgrades to endpoint protection. • Migrated to a new server hosting infrastructure with enhanced technical and physical safeguards. • Enhanced backup and disaster recovery capability. • Implemented two-factor authentication. • Improved staff training on password policies and best-practices. Training will include review of policies and procedures. • Ongoing technical and administrative improvements may be implemented based on recommendation from contractors.
Steps taken to notify individuals of the incident	Affected employees were notified by letter on April 23, 2021. Affected patients were notified by letter between June 14 and August 11, 2021. In addition, 329 referring physicians were notified by letter between June 14 and August 11, 2021.
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: *Possible harm that may result from unauthorized access or disclosure of employee personal information may include fraud, identity theft, exposure to phishing campaigns or attempts to obtain further personal information. The Organization has no evidence at this time that any specific harm has occurred.* *Possible harm that may result form [sic] unauthorized access or disclosure of patient information may include loss of confidentiality, personal embarrassment, and damage to reputation. The Organization has no evidence at this time that any specific harm has occurred[.]* I agree with the Organization's assessment. A reasonable person would consider the contact, identity, financial (tax, RRSP forms), and employment information (agreements, payroll information) at issue could be used to cause the harms of identity theft, fraud, and increased exposure to phishing. Employment information (employee evaluations) could also be used to cause the harms of embarrassment, hurt or humiliation,

	damage to reputation or relationships, or loss of employment, business or professional opportunities. Patient identity and medical information (procedure type and result) could be used to cause the harms of embarrassment, or damage to reputation or relationships. The above, in combination with other sources of contact information and knowledge that a patient received services from the Organization, increases exposure to the possible harms of phishing and therefore, fraud and identity theft. All of the above 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: *The likelihood of harm to employees is moderate. The information that was was* [sic] *exfiltrated was taken as a result of a malicious act. Because the information included financial information and contact information, there is a reasonable risk that the hacker could attempt to use the information for malicious purposes including theft, fraud or identity theft.* *The likelihood of harm to patients is low. While the information is personally sensitive, it has little commerical* [sic] *value. The primary aim of Sodinokibi attacks is financial gain. The categories of information are not those which create a risk of identity theft or financial loss. The potential harm is personal and could cause embarrassment* [sic] *if further disclosed. However, the hacker obtained no information that could be used to try to contact or extort affected individuals with the sensitive information.* Additionally: "The Organization has no evidence at this time that any specific harm has occurred." I accept the Organization's assessment. 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, exfiltration of records, deployment of ransomware). Despite the "primary aim of Sodinokibi attacks [being] financial gain", presumably from ransom payment, personal information was nonetheless compromised and can be used in combination with other breaches or open-sources of information to cause harm.

	A lack of evidence that harm has occurred does not mitigate against the possibility of harms from occurring in the future.

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, identity, financial (tax, RRSP forms), and employment information (agreements, payroll information) at issue could be used to cause the harms of identity theft, fraud, and increased exposure to phishing. Employment information (employee evaluations) could also be used to cause the harms of embarrassment, hurt or humiliation, damage to reputation or relationships, or loss of employment, business or professional opportunities.

Patient identity and health information (procedure type and result) could be used to cause the harms of embarrassment, or damage to reputation or relationships. The above, in combination with other sources of contact information and knowledge that a patient received services from the Organization, increases exposure to the possible harms of phishing and therefore, fraud and identity theft.

All of the above are 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, exfiltration of records, deployment of ransomware).

Despite the "primary aim of Sodinokibi attacks [being] financial gain", presumably from ransom payment, personal information was nonetheless compromised and can be used in combination with other breaches or open-sources of information to cause harm.

A lack of evidence that harm has occurred does not mitigate against the possibility of harms from occurring in the future.

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).

I understand the Organization notified affected individuals by letter on April 23, 2021, and June 14 – August 11, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner