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	NorthShore University HealthSystem (Organization)
Decision number (file number)	P2020-ND-116 (File #017210)
Date notice received by OIPC	September 4, 2020
Date Organization last provided information	September 16, 2020
Date of decision	October 2, 2020
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 is an integrated healthcare delivery system primarily serving individuals in the greater Chicago area in Illinois, 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: • full name, • date of birth, • address, • telephone number, • email address, and • giving history (i.e. donation dates and amounts). 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, I have jurisdiction in this matter. The Organization reported that no credit card, bank account information, social insurance numbers, or user login credentials and passwords were compromised or accessed. To the extent, such information is ever retained by the Organization's service provider, it is encrypted. Further, as the affected Canadian

	individuals were donors, not patients, no health related information was impacted.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization uses a third-party service provider, Blackbaud, who provides a platform to manage donor information. • On July 22, 2020, the Organization received a notice from Blackbaud reporting that cybercriminals obtained access to information Blackbaud processed for the Organization. • Blackbaud advised the Organization that it paid a financial demand in exchange for confirmation from the attackers that the extracted information was destroyed. • The incident occurred between February 7 through May 20, 2020.
Affected individuals	The incident affected 335,484 individuals of which 3 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	The Organization reported its service provider: • Notified law enforcement. • Locked out the unauthorized user. • Engaged a third party to monitor the dark web to ensure there is no misuse of the accessed data. • Heightened its security efforts to better protect against future ransomware attacks. • Paid a financial demand in exchange for confirmation that the extracted information was destroyed. The Organization: • Notified affected individuals. • Notified the Privacy Commissioner of Canada. • Advised affected individuals of precautions that can be taken to reduce the risk of harm.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on September 4, 2020.

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 information potentially impacted for individuals in Canada consisted of name, date of birth, contact information and giving history. While these are not particularly sensitive data fields, we note the incident arose from malicious actors (ransomware), and there is a potential for this information to be used for identity theft, spear phishing, fraud, and other crimes, or public disclosure of private information.* I agree with the Organization's assessment. A reasonable person would consider that email address, contact and profile information (donation history, etc.) could be used for phishing, increasing vulnerability to identity theft and fraud. 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: *The incident was caused by the ransomware, which is used by criminal undertakings. The service provider impacted by the breach informs us that they paid a financial demand from the attackers in exchange for confirmation from them that the extracted information was destroyed. This and the lower sensitivity of the Canadian information impacted lower the likelihood of harm materializing so, we would assess the overall risk as low.* In my view, a reasonable person would consider the likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate, unauthorized action, ransom demand). The Organization reported that the personal information of donors was both accessed and stolen and the Organization cannot confirm the information will not be misused, disseminated or otherwise made available publicly.
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 email address, contact and profile information (donation history, etc.) could be used for phishing, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to malicious intent (deliberate, unauthorized action, ransom demand). The Organization reported that the personal information of donors was both accessed and stolen and the Organization cannot confirm the information will not be misused, disseminated or otherwise made available publicly.

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 the affected individuals in a letter dated September 4, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner