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	Canadian Blood Services (Organization)
Decision number (file number)	P2017-ND-137 (File #005298)
Date notice received by OIPC	March 28, 2017
Date Organization last provided information	September 18, 2017
Date of decision	October 3, 2017
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates on a not for profit basis. 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. "Non-profit organization" is defined in section 56(1) to mean an organization "that is incorporated under the *Societies Act* or the *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act*." In this case, the Organization is incorporated under the federal *Canada Not-for-Profit Corporation Act* and does not qualify as a "non-profit organization" as defined in section 56(1)(b) of PIPA, despite operating on a not for profit basis. I have jurisdiction because the Organization 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, • email address, • affiliation with a specific academic institution, • donor identification number, and • medical history. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On March 4, 2017, a donor with the Organization submitted a request to the Organization's National Contact Center for a change to her ethnicity and gender. • When forwarding the request by email to an internal department for response, an employee with the Organization mistakenly included an additional external email address in the addressee field. • The unintended recipient notified the Organization of the error on March 9, 2017. • The Organization contacted the unintended recipient and asked that the email sent in error be deleted from her email inbox and trash folders; however, the Organization did not receive confirmation that this was done. • The unintended recipient requested that the Organization remove her from its email contact list, which was done. The Organization attempted no further contact with the unintended recipient.
Affected individuals	The incident affected one (1) Alberta resident.
Steps taken to reduce risk of harm to individuals	• Requested that the email at issue be deleted from the unintended recipient's email inbox and trash folders. • Removed the unintended recipient from the Organization's email contact list, as requested. • Conducted a risk assessment and notified this office.
Steps taken to notify individuals of the incident	The affected individual was notified by telephone on March 22, 2017.

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 did not identify any specific harm that might result from this incident but reported it "has conducted a risk assessment and … there may be a risk of harm to the individual due to the sensitive nature of the information." In my view, the sensitive medical information at issue could be used to cause hurt, humiliation, and embarrassment. These are significant harms. Email address could be used to send unsolicited emails and for phishing, which I have previously found to be a significant harm.
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 specifically address the likelihood of harm resulting from this incident but, as noted above, reported it "has conducted a risk assessment and … there may be a risk of harm to the individual due to the sensitive nature of the information." In my view, a number of factors reduce the likelihood of harm resulting in this case, including that the incident resulted from human error and not malicious intent, the unintended recipient reported the breach to the Organization, and there does not appear to be a personal/professional relationship between the affected individual and the unintended recipient. Nonetheless, and considering the sensitivity of the information at issue in this case, I am concerned that the Organization was not able to confirm the email was destroyed and not forwarded to other parties, despite a number of attempts to do so.

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 individual.

The sensitive medical information at issue could be used to cause hurt, humiliation, and embarrassment. These are significant harms. Email address could be used to send unsolicited emails and for phishing, which I have previously found to be a significant harm. A number of factors reduce the likelihood of harm resulting in this case, including that the incident resulted from human error and not malicious intent, the unintended recipient reported the breach to the Organization, and there does not appear to be a personal/professional relationship between the affected individual and the unintended recipient. Nonetheless, and considering the sensitivity of the information at issue in this case, I am concerned that the Organization was not able to confirm the email was destroyed and not forwarded to other parties, despite a number of attempts to do so.

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

I understand the Organization notified the affected individual by telephone on March 22, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner