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	College and Association of Registered Nurses of Alberta (Organization)
File number	P2017-ND-06 (File #002661)
Date notice received by OIPC	March 31, 2016
Date Organization last provided information	March 31, 2016
Date of decision	January 4, 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 is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • Front image of a driver's license (name, address, date of birth, photograph, signature, physical description, driver's license number); • Data page of passport (name, date of birth, nationality, place of birth, passport number, photograph, signature); • Email address, • Employment information (name of employer, office telephone number, position). This information is about an identifiable individual 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 February 10, 2015, a Registration Assistant with the Organization emailed copies of a member's driver's license, passport, and communication thread to the wrong individual. • The unintended recipient contacted the Organization on February 17, 2016, one year later, and reported the error. • The unintended recipient confirmed she destroyed copies of the original email and attached documents. • The email was sent without a password or encryption.
Affected individuals	The incident affected one (1) individual.
Steps taken to reduce risk of harm to individuals	• Verbally confirmed the unintended recipient deleted the original email and did not make copies. • Investigating use of encryption for sensitive emails.
Steps taken to notify individuals of the incident	The Organization notified the affected individual by email sent March 30, 2016.
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 that "There is the potential for identity theft …". I agree with the Organization's assessment. The personal information at issue includes comprehensive and sensitive identity information that could be used to cause the harms of identity theft and fraud. The email address could be used for phishing purposes. 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 that "Our assessment of harm is low due to the fact that the unintended recipient advised us of the error and confirmed the deletion the information [sic]. There were no language barriers and the individual understood our instructions to destroy the information. If the information had been compromised the intended recipient would probalby [sic] be aware by now." I generally agree with the Organization's assessment. The incident was the result of human error, and the unintended recipient reported the matter to the Organization and confirmed the information was deleted and not copied; these factors reduce the likelihood of harm resulting from this incident. However, I am concerned that the incident was not reported to the Organization for over one year. In my view, the length of time the personal information was exposed increases the likelihood of harm.

DECISION UNDER SECTION 37.1(1) OF PIPA
Given the information reported by the Organization, I have concluded that there is a real risk of harm to the affected individual in this case. The personal information at issue includes comprehensive and sensitive identity information that could be used to cause the harms of identity theft and fraud. The email address could be used for phishing purposes. These are significant harms. The incident was the result of human error, and the unintended recipient reported the matter to the Organization and confirmed the information was deleted and not copied; these factors reduce the likelihood of harm resulting from this incident. However, I am concerned that the incident was not reported to the Organization for over one year. In my view, the length of time the personal information was exposed increases the likelihood of harm. I require the Organization to notify the affected individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the affected individual by email sent March 30, 2016. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner