

INTERPRETATION BULLETIN

Personal Health Information Privacy and Access Act Subsection 49(2) – Privacy Breach Notification

August 11, 2011

Office of the Access to Information and Privacy Commissioner of New Brunswick

This **Interpretation Bulletin** is issued by the Access to Information and Privacy Commissioner ("the Commissioner") under the authority of the *Personal Health Information Privacy and Access Act* ("the Act"). The Commissioner issues Interpretation Bulletins as questions of interpretation of this legislation arise.

The purpose of this **Interpretation Bulletin** is to provide the Commissioner's interpretation of subsection 49(2) and its effect upon the notification obligations found in paragraph 49(1)(c) of the Act. In particular, the interpretation is to guide custodians on which instances it is necessary to notify the Commissioner and those individuals where there has been a breach in the handling of their personal health information.

PRIVACY BREACH NOTIFICATION

Section 49 of the Act provides as follows:

- 49(1) A custodian shall...
- (c) notify the individual to whom the information relates and the Commissioner in the manner prescribed by the regulations at the first reasonable opportunity if personal health information is
 - (i) stolen,
 - (ii) lost,
 - (iii) disposed of, except as permitted by this Act, or
 - (iv) disclosed to or accessed by an unauthorized person...
- 49(2) Paragraph 1(c) does not apply if the custodian reasonably believes that the theft, loss, disposition, disclosure or access of personal health information will not
- (a) have an adverse impact on the provision of health care or other benefits to the individual to whom the information relates,
 - (b) have an adverse impact on the mental, physical, economic or social well-being of the individual to whom the information relates, or
 - (c) lead to the identification of the individual to whom the information relates.

COMMISSIONER'S INTERPRETATION

The Act is founded on the principle that personal health information is highly sensitive and represents an individual's most private information. People must confide their personal health information in order to access a multitude of services from the health care system and in exchange, these individuals trust health care providers to treat their private information with the utmost respect and confidentiality.

The Act applies to all health care custodians, including individuals or organizations that collect, maintain or use personal information for one or more of the following purposes:

- (a) providing or assisting in the provision of health care or treatment,
- (b) planning and the management of the health care system, or
- (c) delivering a government program or service.

The mandatory breach notification provision found in paragraph 49(1)(c) requires that all custodians notify, at the first reasonable opportunity, the individuals affected by the breach as well as the Commissioner when it is discovered that personal health information has been compromised. A breach event includes a case where personal health information has been lost, stolen, disposed of in an unauthorized manner, or disclosed to or access by an unauthorized person.

There are both public and private sector custodians.

Public sector custodians include, among others:

- public bodies
- the Department of Health
- Regional Health Authorities and hospitals, health centres under their authority
- the New Brunswick Health Council
- Ambulance New Brunswick
- Facilicorp NB Ltd.
- the Workplace Health, Safety and Compensation Commission
-

Private sector custodians include, among others:

- Health care providers:
 - o Doctors
 - o Nurses
 - o Dentists
 - o Physiotherapists
 - o Psychologists
- Health care facilities
 - o Special care homes
 - o Medical clinics
- Nursing homes
- Laboratories and blood or other specimen collection centres

As the Act obligates custodians to protect personal health information entrusted to them, and given the highly sensitive nature of personal health information, individuals have the right to know when their information has been compromised. Therefore, the mandatory privacy breach notification rules found in section 49 become an additional mechanism for custodians to remain accountable in cases where a breach has taken place when handling personal health information entrusted to them. The notification process will enable custodians to reduce the risk of harm for those individuals whose personal health information was compromised.

For these reasons, the privacy breach notification is obligatory and can only be disregarded in specific limited circumstances as set out in subsection 49(2). The Commissioner interprets subsection 49(2) to signify that if a privacy breach event has taken place, it is meant to trigger a risk assessment on the part of the custodian to determine whether the individual whose private information was compromised may be at an increased risk of harm as a direct result of the privacy breach.

The Commissioner interprets this provision to mean that if any of the three types of harm to individuals referred to in subsection 49(2) may occur as a result of the privacy breach - and that it is reasonable to so believe given the facts surrounding the breach - then the custodian must notify. The facts of the breach must be assessed by the custodian as it is important to point out that in all cases, the onus remains on the custodian to establish why notification was not believed to be necessary.

Consequently, a custodian can only discount the mandatory rule to notify the individual whose personal health information has been the subject of a breach in a case where the custodian reasonably believes, given the facts surrounding the incident, that the breach:

- (a) will not affect the care (or benefits) to be provided to the individual,
- (b) will not affect the mental, physical, economic or social well-being of the individual,
and
- (c) will not lead to the identification of the individual.

In other words, the custodian can only forego the notification obligation when the custodian has a reasonable belief that none of the three possible risks of harm referred to above could exist as a result of the privacy breach.

To illustrate this point, consider two similar scenarios which present two different notification outcomes.

Scenario 1

A custodian leaves a briefcase containing medical files of her patients in her locked car parked on the side of the street. She forgets to take the briefcase inside her office that day. The briefcase is locked. The car is broken into and a number of items are stolen, including the briefcase. The briefcase is found a few hours later just around the corner. The lock on the briefcase is neither broken nor shows signs of tampering. This is a case of stolen personal health information. The custodian assesses the situation before deciding whether she needs to notify of the breach. Based on these facts, she can fairly state that the medical files were never read, copied or taken, and as a result, she can reasonably believe that the breach (the theft) will not affect the care or benefits to be provided to her patients, will not affect the mental, physical, economic or social well-being of her patients, and will not lead to the identification of her patients. In this fact scenario, none of the three types of harm could exist, and the custodian is correct in not having to notify her patients or the Commissioner.

Scenario 2

A custodian leaves a briefcase containing medical files of his patients in his locked car parked at home. The briefcase is not locked. During the night, the car is broken into and a number of items are stolen, including the briefcase. The briefcase is found a few hours later just around the corner. The briefcase does not show signs of tampering, but given that it was not locked, it is difficult to state whether it was opened and the contents viewed. This is a case of stolen personal health information. The custodian assesses the situation before deciding whether he needs to notify of the breach. Based on these facts, he cannot reasonably be sure that the medical files were never read, but he can probably ascertain that they were not copied or taken if all records are intact. In this particular set of facts, the custodian may fairly state that the breach (the theft) will not affect the care or benefits to be provided to his patients, will not affect the mental, physical, economic or social well-being of his patients. The custodian cannot, however, reasonably believe that the theft will not lead to the identification of his patients because the thief may have viewed the contents of the unlocked stolen briefcase. In this fact scenario, one of the possible harm does exist and the custodian must accordingly notify both his patients and the Commissioner.

The *Act* therefore in many circumstances surrounding privacy incidents obligates custodians to notify affected individuals and the Commissioner of breaches of personal health information. The Commissioner also encourage custodians to contact our Office as soon as they become aware of either an actual or a suspected privacy breach for the reasons that this will provide an opportunity for her Office to provide guidance and assistance in the handling of the privacy

breach. This assistance will ensure that proper safeguards are put in place to reduce the risk of reoccurrences.

The Office has developed a **Privacy Breach Reporting** form for custodians that is designed to assist custodians and the Commissioner in identifying the cause of the breach, in assessing the risk of harm, and in containing the breach in matters of privacy breach incidents. For convenience, the form is attached to this **Interpretation Bulletin**.

The Office of the Commissioner views the privacy breach notification process as an integral component to the successful implementation of the *Act* through the education of the requirements of the *Act*, and as an equally essential component to the building of trust relationships which must exist between health care providers and the public.


If you require more information about the above, please contact us at:

65 Regent Street, Suite 230

Fredericton, NB

E3B 7H8

 506.453.5965 (Toll Free: 1.877.755.2811)

 506.453.5963

 access.info.privacy@gnb.ca