

The *Personal Health Information Act* Risk Management Toolkit

Privacy Breach Guidelines

Introduction

The Newfoundland and Labrador *Personal Health Information Act* (PHIA) sets out the rules that persons or organizations defined as custodians of personal health information must follow when collecting, using, disclosing, retaining and disposing of personal health information.

PHIA recognizes the unique character of personal health information as being extremely sensitive and also recognizes that it is frequently collected, used and disclosed for a variety of authorized purposes. These purposes include care and treatment, health research, quality control and risk management.

PHIA balances individuals' right to privacy with respect to their own personal health information with the legitimate needs of health information custodians to collect, use and disclose this information. With certain limited exceptions, PHIA requires custodians of personal health information to obtain consent before they collect, use or disclose the information in their custody or control. PHIA also makes custodians responsible for the secure storage and destruction of personal health information. Additionally, individuals have the right to access and request correction of their own personal health information.

The purpose of this document is to provide guidance to custodians when they are faced with a privacy breach.

What is a privacy breach?

A privacy breach is any collection, use or disclosure of personal health information that is not authorized under PHIA. In essence, a privacy breach occurs whenever a person has contravened or is about to contravene a provision of PHIA, or of the regulations passed under PHIA.

As an example, section 15 of PHIA requires that custodians take steps that are reasonable in the circumstances to ensure personal health information in their custody or control is:

- (1) Protected against theft, loss and unauthorized use or disclosure,
- (2) Retained, transferred and disposed of in a secure manner; and,
- (3) Protected against unauthorized copying, modification or disposal.

A failure to meet these requirements represents some of the more common circumstances under which a privacy breach could arise. Again, however, it is

important to bear in mind that any collection, use or disclosure of personal health information which is not in accordance with the PHIA could also be considered a breach.

A custodian of personal health information may become aware of a privacy breach in a number of ways. It is frequently the case that a custodian may itself identify a breach during the normal course of its business or operations. A custodian may also be contacted by the Newfoundland and Labrador Office of the Information and Privacy Commissioner (NL OIPC) if a concern about its operations has been raised by a member of the public. Finally, the NL OIPC could initiate its own investigation if it determined that such was in the public interest.

This appendix will focus primarily on situations where a custodian has itself identified a privacy breach or where the custodian has been contacted by the NL OIPC regarding a potential breach. Such situations often arise where personal health information has been stolen, lost or accessed by unauthorized persons. Many of these situations will involve unintentional breaches of PHIA. For example, personal health information may be lost (a patient's file is misplaced), stolen (laptop computers are a prime example) or inadvertently disclosed to an unauthorized person as a result of an honest mistake (a letter addressed to patient A is actually mailed to patient B). However, a custodian may also become aware of breaches that are intentional; for example, an instance where intentional, unauthorized access of patient files by staff has occurred.

Where a privacy breach has occurred, custodians are encouraged to contact the NL OIPC so that assistance can be provided to the custodian in fulfilling its obligations under PHIA (e.g. notification of persons involved) and in taking whatever steps might be necessary to prevent similar occurrences in the future.

The Benefits of Having a Privacy Breach Protocol

It is recommended that a custodian of personal health information develop a privacy breach "protocol", or a process for systematically responding to privacy breaches. A privacy breach protocol should include provisions for addressing all of the actions outlined in this document. Having a privacy breach protocol in place *before* an adverse privacy event occurs is strongly advised; this will yield several benefits:

- Custodians can respond quickly and in a coordinated manner;
- Roles and responsibilities of staff will be understood beforehand;
- A process for effective investigations will be documented and can be set into motion;
- Effective containment of the breach will be aided;
- Remediation efforts will be easier; and
- Custodians will be properly prepared for the potential involvement of the NL OIPC.

Health Information Privacy Breach Guidelines

Upon learning of a privacy breach, a custodian must take immediate action. Many of the following guidelines need to be carried out simultaneously or in rapid succession.

Step 1: Containment – Identify the scope of the potential breach and take steps to contain it

- Retrieve the hard copies of any personal health information that has been disclosed;
- Ensure that no copies of the personal health information have been made or retained by the individual who was not authorized to receive the information and obtain the person's contact information in the event that follow-up is required; and,
- Determine whether the privacy breach involved unauthorized access to any other records of personal health information (e.g., an electronic information system) and take whatever steps are necessary and appropriate (e.g., change passwords, identification numbers and / or temporarily shut down a system) to prevent further breaches from occurring.

Step 2: Evaluate – Respond immediately by implementing the privacy breach protocol

- Ensure appropriate staff within your organization are immediately notified of the breach, including the Chief Privacy Officer or the designated contact person for the purposes of the Act;
- Depending on the nature or seriousness of the privacy breach, there may be a need to contact senior management, patient relations or the information and technology and/or communications department within your organization;
- Depending on the nature or seriousness of the privacy breach, there may be a need to inform the NL OIPC of the privacy breach and work together constructively with its staff (see section 15(4) of PHIA); and
- Address the priorities of containment and notification as set out in the following steps.

Step 3: Notification – Identify those individuals whose privacy was breached and notify them of the breach

Any individuals whose information was the subject of a privacy breach **must be notified, unless certain criteria are met**. Specifically, there is **no** requirement under PHIA to notify those individuals where the theft, loss,

unauthorized disposition, or improper disclosure or access of their personal health information will not have an adverse impact on either:

1. the provision of health care or other benefits to the individual who is the subject of the information; or,
2. the mental, physical, economic or social well-being of the individual who is the subject of the information

Otherwise, PHIA requires health information custodians to notify individuals of the breach at the first reasonable opportunity.

Regarding notification:

- PHIA does not specify the manner in which notification must be carried out. However, for example, notification can be by telephone or in writing, or depending on the circumstances, a notation made in the individual's file to be discussed at their next appointment;
- There are many factors that may need to be taken into consideration when deciding on the best form of notification (e.g., the sensitivity of the personal health information). As a result, the health information custodian may want to contact the NL OIPC to discuss the most appropriate form of notification;
- There may also be exceptional circumstances when a custodian may want to discuss notification with the NL OIPC before proceeding; for example, when notification is not reasonably possible or may be detrimental to the individual. In cases such as these, the health information custodian is encouraged to contact the NL OIPC to discuss the circumstances and potential approaches to notification;
- When notifying individuals affected by the breach, custodians should provide details of the extent of the breach and the specifics of the personal health information involved in the breach;
- Custodians should advise affected individuals of the steps that have been or will be taken to address the breach, both immediate and long-term;
- Custodians should advise affected individuals that the NL OIPC has been contacted to ensure that all obligations under the Act are fulfilled, where applicable (certain circumstances actually require custodians to notify the NL OIPC about a breach – see section 15(4) of PHIA); and,
- Custodians should advise affected individuals that those individuals may contact the NL OIPC directly if they are not satisfied with the measures taken by the custodian to respond to the breach.

Step 4: Investigation and Prevention

- Conduct an internal investigation into the matter. The objectives of an internal investigation are to:
 - ensure the immediate requirements of containment and notification have been addressed;
 - review the circumstances surrounding the breach; and
 - review the adequacy of existing policies and procedures in protecting personal health information.
- Address the situation at a systemic level. In some cases, program-wide procedures may warrant review (e.g., responding to telephone inquiries from family members regarding patients or clients);
- Advise the NL OIPC of your findings and work together with that Office to make any necessary changes;
- Ensure staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of PHIA; and,
- Cooperate in any further investigation into the incident undertaken by the NL OIPC.

What happens when the Commissioner investigates a privacy breach?

When investigating a privacy breach, depending on the circumstances, the NL OIPC may:

- Ensure any issues surrounding containment and notification have been addressed;
- Interview individuals involved with the privacy breach or individuals who can provide information about a process;
- Obtain and review the health information custodian's position on the privacy breach;
- Ask for a status report of any actions taken by the health information custodian;
- Review and provide input and advice on current policies and procedures and any other relevant documents and recommend changes; and,
- Where appropriate or necessary, issue a Report containing recommendations at the conclusion of the review.

Steps custodians can take to avoid a privacy breach

Custodians governed by PHIA are strongly urged to proactively adopt measures to prevent privacy breaches from occurring. These measures would normally include:

- Ensuring that policies and procedures are in place that comply with the privacy protection provisions of PHIA and that staff are properly trained in this respect;
- Safeguarding personal health information when it is physically removed from the office or institution; for example, by ensuring that all laptops and PDA's are password protected and data is encrypted;
- Ensuring that a baseline of logging and auditing is in place on all systems, particularly those containing electronic health records and that staff are aware that regular audits will occur;
- Conducting a privacy impact assessment (PIA) where appropriate. The PIA is a process that helps determine whether new technologies, information systems and proposed programs or policies meet basic privacy requirements (For further assistance with PIAs, see the "Privacy Impact Assessment Guidelines for the Newfoundland and Labrador *Personal Health Information Act*", available on the Department of Health and Community Service's website);
- When in doubt, obtaining advice from your organization's legal department and/or Chief Privacy Officer; and,
- Encouraging a culture of privacy within your organization.