Eastern Health

Submission to the Personal Health Information Review Committee

February 2017

TABLE OF CONTENTS

A. EXECUTIVE SUMMARY

Eastern Health's submission to the PHIA Review Committee identifies what is currently working well with the *Personal Health Information Act* ("PHIA") and where improvements are needed. For areas where improvements are needed, this submission identifies the key issues, provides an analysis of each issue, and puts forth a suitable resolution. The analysis of each issue described is primarily concerned with the implications and outcomes as experienced by a Regional Health Authority, but the implications identified in analysis apply to all custodians. The following areas of importance were identified:

- privacy breaches
- oath/affirmation
- custodian definition
- health research
- prosecution timelines
- fees for release of information
- timeline for a custodian to reply to a complaint
- response of a custodian to a report

For clarity, the relevant sections of PHIA or the *Personal Health Information Regulations* ("Regulations") that correspond with an issue discussed are identified. The sections of PHIA referenced in this document can be found in Appendix A, while those sections relating to the Regulations can be found in Appendix B.

Eastern Health is the largest integrated health organization in Newfoundland and Labrador. We provide the full continuum of health services to a regional population of more than 300,000 and are responsible for a number of unique provincial programs. Our over 13,000 health care and support services professionals believe in providing the best quality of care and health service delivery in our region and in the province. Eastern Health extends west from St. John's to Port Blandford and includes all communities on the Avalon, Burin, and Bonavista Peninsulas.

PHIA was proclaimed into force on April 1st, 2011, and is a health-sector specific privacy law that establishes rules that custodians of personal health information ("Information") must follow when collecting, using and disclosing individuals' confidential Information. PHIA also sets out the rights of residents of the province regarding obtaining access to and exercising control of their Information. Upon proclamation, Eastern Health became a custodian under PHIA and was, accordingly, required to adhere to the rules established under PHIA. Since the proclamation of PHIA, Eastern Health has been devoted to observing the provisions of PHIA. Eastern Health, as the largest custodian in Newfoundland & Labrador, appreciates the opportunity to submit feedback on issues and improvements regarding PHIA.

B. WHAT IS CURRENTLY WORKING WELL WITH PHIA

In the five years since the proclamation of PHIA, it has proven to be beneficial and valuable legislation, and there are many areas where PHIA is working well. Here are but a few.

B.1. PROVISIONS REGARDING THE COLLECTION, USE, AND DISCLOSURE OF INFORMATION

Value: Establishes parameters regarding the collection and use, and permits latitude regarding the disclosure, of Information.

PHIA establishes provisions on the collection, use, and disclosure of Information in the custody or control of a custodian. For example, PHIA outlines where the collection of Information must occur with consent, circumstances under which indirect collection may occur, how much Information can be collected, permitted uses of the Information, disclosure of Information, and so on. Having such provisions explicated outlined in legislation is beneficial for custodians.

With respect to disclosure, under the current wording of PHIA, custodians have a certain amount of latitude with respect to disclosure without consent of Information such as but not limited to disclosure related to health and safety, related to proceedings, for research purposes, or of registration information. This latitude afforded custodians is beneficial, because it permits for planning or delivering health care programs or services provided, for the processing, monitoring, verifying, or reimbursing claims for payment for the provision of health care, etc.. While obtaining explicit consent from the person who is the subject of the Information is prudent and a best practice, there are times when the obtainment of consent can be burdensome. Because of this, PHIA included the aforementioned provisions for custodians.

Resolution: Maintain the current provisions regarding collection, use, and disclosure of Information for custodians.

B.2. EMPLOYEE OBLIGATIONS

Value: Establishes an equal and minimum requirement for employees of all custodians.

Another strength of PHIA is that, in addition to placing parameters around the collection, use, and disclosure of Information, it outlines obligations that a custodian must ensure its employees, health care professionals, agents, contractors, and volunteers attain. Two of these obligations are to take

an oath or affirmation, and being aware of the duties imposed by PHIA and the regulations, which is best attained by the completion of training.

As an oath or affirmation is a promise to hold true the contents of the oath or affirmation based on personal honor, it is a very beneficial requirement. The taking of an oath or affirmation reinforces the significance and special trust placed in health-care sector employees by the patients/clients/residents who utilize those services, and it provides guidance against any abuse of that trust. Additionally, privacy training provides the basis for a "human firewall" against Information loss and increases awareness of risks to patients' well-being. So, like the taking of the oath or affirmation, requiring that training be completed is very beneficial.

Resolution: Maintain the current requirements that an oath or affirmation be taken, and that training be completed.

B.3. PRIVACY BREACH NOTIFICATION/REPORTING

Value: Establishes the criteria for when notification/reporting is required.

Notification regarding privacy breaches is beneficial, in that it better informs and protects individuals who may be the subject of a privacy breach, and it highlights to a custodian the importance of adhering to the requirements to protect privacy. In the event of a material privacy breach, notification to both the person who is the subject of the Information and the OIPC must occur, as per the requirements of PHIA. Eastern Health ardently adheres to the current requirements of PHIA and can attest that the current notification requirements in PHIA are sufficient.

Resolution: Maintain the current requirement of notifying in the event of a material breach.

C. WHERE IMPROVEMENTS ARE NEEDED

C.1. PRIVACY BREACHES

C.1.1. Material Breach Definition

Issue: Ambiguity and confusion with the definition of "material" as outlined in PHIA.

Subsection 15(4) outlines the requirements for when a custodian determines that a privacy breach has occurred. Eastern Health diligently adheres to these requirements and makes every effort to complete the notification process in a reasonable time period. However, the process is not without challenges. Under the current wording, the OIPC is to be notified when a privacy breach is deemed to be material "…as per the regulations…" Section 5 of the Regulations outlines a number of criteria to be used to determine if a breach is material in nature. However, this results in a latitude of discretion with respect to determining when a breach is material.

Improving the definition of material in the regulations may reduce this level of latitude in discretion. An improved definition can lead to improved privacy and human resources practices. The consistent approach will provide a standard methodology to custodians when processing material breaches.

Additionally, the current national climate regarding breach notification is to notify when it has been determined there is risk of serious harm[1,2]. Given PHIA requires notification in the event of a material breach, current practices are harmonized with the national practices and requirements. We believe that modifying PHIA to address the issues regarding the definition of material breach will better enable custodians to remain consistent.

Resolution: Provide an expanded and more detailed definition of "material", and consider issuing guidance and education on when a breach is material.

[1] https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11177.html#s1.2
[2] http://www.oba.org/en/pdf/sec_news_pri_jan12_kar_bre.pdf

C.1.2. Wording of Notification Protocol

Issue: Use of double negative wording regarding notification protocol highlights, which results in ambiguity and confusion notification.

Further complicating the notification process is the fact that there is a double negative regarding harm and notification. In addition to identifying the circumstances under which notification must occur, PHIA also identifies the circumstances under which notification may not be appropriate. However, double negative wording is used in ss. 15(7). In determining if notification must occur, custodians need to balance promptness with the possible impact of harm to the person who is the subject of the Information, and it would appear that such was the intent for ss.15(7). That is, the intent for ss.15(7) was to identify when notification could be delayed or would not be required. However, having double negative wording in ss.15(7) is counterintuitive to this intent. For example, according to the above, if there will not be an adverse impact upon an individual's mental, physical, or social well-being, then a custodian does not have to notify them. To put in it another way, this section appears to be saying that a custodian must notify when such notification will cause harm. That doesn't seem right.

Shouldn't it be that notification is not required when it is reasonably believed that such notification could result in an adverse impact on the individual who is the subject of the Information?

Resolution: Provide clear and concise wording regarding notification. Consider the wording to be such that notification will not be required when it is reasonably believed that such notification may result in an adverse impact on the individual who is the subject of the Information.

C.2. OATH/AFFIRMATION

Issue: Requirements regarding the oath/affirmation.

As mentioned in section B, the taking of an oath/affirmation is beneficial. However, in its current wording, the only requirement in PHIA regarding oaths or affirmations is that a custodian must ensure that its employees, etc. take one. There are no requirements regarding the acquisition of a signed oath or affirmation or in what form (i.e. written or verbal) the oath or affirmation must be.

Additionally regarding the current wording, there is the requirement that all contractors take an oath or affirmation. This is problematic, as not all contractors are privy or exposed to Information, nor are all contractors locally based. For example, a contractor who provides office supplies would most likely not be privy to or interact with Information. However, under the current wording for PHIA, this contractor must take an oath or affirmation.

Resolution: That an oath or affirmation be in written form (e.g. being in written or electronic form permits for better tracking, it is tangible, etc.) and signed, and that a level of latitude be afforded custodians with respect to ensuring all contractors shall take an oath.

C.3. CUSTODIAN DEFINITION

C.3.1. Ambiguity with the Term Custodian

Issue: Who is the proper custodian with respect to secondary uses of Information.

Subsection 4(1) of PHIA provides interpretation for the word custodian. While the current interpretation is extensive, there is ambiguity with the application of the term 'custodian' with respect to secondary uses of data. Eastern Health is listed as a custodian, as is a health care provider. But who is the custodian when it comes to use or disclosure of Information when, based on PHIA, both Eastern Health and the health care provider are the custodians? The provision in PHIA regarding the disclosure of Information for health research purposes is discretionary and is directed to the custodian. So, it doesn't abscond the issue of who is the proper custodian.

For example, an initiative (and we can assume that the appropriate approvals have been obtained, whatever those approvals are) is wanting Information (e.g. blood work results, physician notes, etc.). The Information is housed on the Meditech system of Eastern Health, which means the Information is in the custody and control of Eastern Health. However, but for a physician[3] requested the testing or wrote the reports that are in Meditech, there wouldn't be any Information in Meditech, therefore the physician is also a custodian of that particular piece of Information. This presents a conundrum, because the requirements regarding collection, use, and disclosure are directed at the custodian. That is, according to

[3] The physician in this example is not an employee of Eastern Health but is fee-for-service.

PHIA, as both Eastern Health and the physician are custodians of the Information, both would need to be involved in any decisions regarding the use or disclosure of Information. Such is not realistic in execution.

From a planning or delivering health care programs or services provided by the Eastern Health perspective, it is important that Eastern Health be able to use the Information in its custody or control. From a health research perspective, it is important that Information be disclosed to researchers. The more streamlined approach to provide Information is via Eastern Health, as it has custody or control over the Information, and it is able to provide a limit of "control" over the Information used or disclosed. Therefore, in such situations, it is essential that Eastern Health be viewed as the custodian and that which will disclose the relevant Information.

Resolution: That there be a provision in PHIA that permits the regional health authority be the primary custodian.

C.3.2. Inclusion Of Post-Secondary Institutions In The Term Custodian

Issue: Limitation of the term custodian to only certain faculties and schools of Memorial University of Newfoundland.

Currently, s.4(1) explicitly lists Memorial University of Newfoundland Faculty of Medicine and Schools of Nursing, Pharmacy, and Human Kinetics and Recreation, as well as Eastern Health's Centre for Nursing Studies, and the Western Regional School of Nursing as custodians. While the aforementioned are involved with health research, there may be more post-secondary institutions were its associated faculty are conducting health research. Additionally, there may be faculties or schools at Memorial that are engaged in or conducting health research. Limiting the application of the term custodian to just the aforementioned faculty and schools precludes the parameters of PHIA from being applicable to all situations.

Resolution: That the definition of custodian include those faculties and schools at post-secondary institutions conducting and involved with health research.

C.3.3. Ensuring That PHIA Is Applicable To All Relevant Organizations

Issue: Not all organizations collecting and using Information are captured by PHIA.

As previously mentioned, PHIA establishes provisions on the collection, use, and disclosure of Information in the custody or control of a custodian, and it outlines a number of responsibilities (e.g. education, taking of an oath, etc.) that a custodian must ensure its employees fulfill. However, there are organizations ("Companies") that collect, use, or disclose the same Information as custodians but are not subject to the provisions of collection, use, and disclosure as prescribed by PHIA, nor are they obligated to ensure that their employees complete certain responsibilities. This presents a problem with respect to Information, as the Information in the custody or control of Companies ought to be subject to the same rigors around collection and use, as well employee responsibilities, as custodians. This would permit assurances to the person who is the subject of the Information.

Broadening the definition of custodian to include Companies may not be the best way to resolve this issue, nor would considering Companies information managers, however, there needs to be a distinction between custodians and Companies regarding the provisions around disclosure without consent. It may not be beneficial to the person who is the subject of the Information if Companies have the same latitude for disclosure as that afforded to custodians. What would be beneficial would be to include in PHIA a term that is less than custodian but more than an information manager whereby Companies would be captured. Moreover, inclusion of such a definition would place Companies under the jurisdiction of the Office of the Information and Privacy Commissioner ("OIPC").

Resolution: That PHIA include a term that is less than custodian but more than an information manager.

C.4. HEALTH RESEARCH

Issue: Omission of health research in the interpretation of Information.

Subsection 5 provides an extensive and inclusive interpretation regarding Information. However, explicitly absent from the interpretation it that Information collected in the purview of health research. Information collected in the purview of health research is just as sensitive as that

Information collected in the clinical setting. The omission of explicitly considering Information collected in the purview of health research as part of the interpretation of section 5 inserts a level of vagueness regarding the application of PHIA to those organizations who engage in health research-related functions. Having health research explicit in section 5 would be beneficial because institutions conducting health research and collecting Information would, as they ought to, be captured by PHIA (as per section C.3.2. of this document.)

Resolution: That PHIA include in the definition of personal health information a provision for health research. (It would be beneficial that a caveat for this provision be that health research is that which requires approval from a research ethics board or research ethics body under the Health Research Ethics Authority Act.)

C.5. PROSECUTION TIMELINES

Issue: Reliance on the Provincial Offences Act to outline prosecution timelines regarding privacy-related offences.

While all breaches are serious offences, there are breaches that occur that warrant prosecution. Currently, PHIA does not outline a timeline with which offences are to be prosecuted. Because of this, charges prosecuted for a PHIA-related offence follow the timelines stipulated in section 7 of the *Provincial Offences Act*, which states:

> *"An information or complaint under this Act may be laid or made before a day 12 months from the day when the matter of the information or complaint arose unless another time limit is provided for in the enactment."*

However, given the nature of privacy breaches, the timeline provisions as stipulated in the *Provincial Offences Act* impede the ability to pursue prosecutory options. It is beneficial for PHIA to address the issue of prosecution in its own right. By doing so, it would not only strengthen PHIA, but it would also bring it in-line with personal health information legislation elsewhere in the country.

Resolution: That PHIA include a section regarding prosecution of PHIA-based privacy breaches.

C.6. FEES FOR RELEASE OF INFORMATION

Issue: Lack of clarity in PHIA regarding application of fees to releasing Information.

The issue of fee application with respect to accessing Information is a bit of a balancing act. On the one hand, the person who is the subject of the Information does have a right to that Information – it is, after all, their Information. However, the Information resides within a record, and given it is the record in the custody or control of a custodian that must be accessed to retrieve the Information, there is a cost to the custodian to accessing the record.

The balance lay with determining what constitutes an appropriate fee. In some situations, requests for Information can be quite large and involve a fair amount of processing on the part of the custodian. Is it fair to expect either the person requesting the Information to pay for the Information or the custodian to absorb the cost of providing the Information? No, not really. It would be fair to expect the person requesting the Information to pay an appropriate fee for it, and it would be fair to expect the custodian to recoup some of the costs associated with processing a request. In its current wording, the charging of fees is discretionary, which permits for variability with respect to not only what is charged but the amount charged. Having the fee costs outlined in PHIA, which would result in consistency among custodians and fairness to the person requesting the Information.

Resolution: That the fees associated with release of information be outlined PHIA.

C.7. TIMELINE FOR A CUSTODIAN TO REPLY TO A COMPLAINT

Issue: Tightness and ambiguity of the timelines regarding a custodian's response to a complaint.

When an individual is notified of a privacy breach, he/she is made aware of the fact that he/she can file a complaint with the Office of the Information and Privacy Commissioner (OIPC). If a complaint is filed with the OIPC, the commissioner contacts the relevant custodian for a response. As per s.69(3), a custodian has fourteen (14) days to produce to the commissioner a copy of the information demanded. Owing to the varied nature of complaints, and that various documents are often requested by the OIPC, compliance to this timeline is challenged. Additionally, the 14 day timeline does not distinguish between calendar days and business days.

Resolution: That timeline for a response to a complaint be twenty (20) business days.

C.8. RESPONSE OF A CUSTODIAN TO A REPORT

Issue: Requirement for a Custodian to send to a complainant written notice of their response to a commissioner's report.

As previously mentioned, an individual can file a complaint with the OIPC in the event his/her Information is breached. If a complaint is filed with the OIPC, the commissioner has the authority to conduct a review of the subject matter of the complaint if the OIPC is satisfied that there are reasonable grounds to do so and will, after concluding the review, prepare a report setting out his or her findings and recommendations. A copy of the report is provided to the complainant and the affected custodian. As per s.74(1), the custodian, within 15 days after receiving a report of the commissioner that contains a recommendation, must give written notice of his or her decision regarding the recommendations to the commissioner and to the complainant.

The above is relatively straight-forward, save for one notable exception, that being that the custodian is required to notify the complainant of the decision in response to the report. The complainant does not file a complaint with the custodian; he/she files it with the OIPC. Any communication involving the custodian pursuant to the investigation by the OIPC is done between the custodian and the OIPC; not between the custodian, the OIPC, and the complainant. In the OIPC complainant process, the custodian is not in contact with the complainant. Therefore, the complainant could be viewed as the OIPC's complainant. Communication to the complainant of the custodian's decision in response to a review should be facilitated by the OIPC.

Resolution: That the OIPC notify a complainant of Eastern Health's response.

D. IMPACT OF CHANGES TO CUSTODIANS AND PATIENTS

While this document is from, and speaks primarily about, Eastern Health, changes to PHIA would impact all custodians (e.g. private physician, physiotherapy, etc. clinics) and patients. Therefore, it is beneficial that consideration be given to the impact on custodians and patients that any changes made may have.

D.1. CHANGES TO THE FREQUENCY OF PRIVACY BREACH REPORTING AND NOTIFICATION

It is worthy to comment on recent trends regarding privacy breach reporting and notification. In recent months, privacy commissioners and review committees across Canada are moving toward mandatory privacy breach reporting and notification regardless of materiality. Implementing changes regarding reporting and notification would not remove the current challenges around such, nor would it serve to heighten the importance of protecting Information.

While custodians are robust in their efforts to adhere to requirements put forth in the legislation, mistakes do occur. Therefore, if mandatory reporting and notification of all breaches were to be required, it would introduce another, possibly more problematic, challenges. For example, at what frequency would such need to occur? The frequency of reporting would negatively impact not only a custodian, as the resource allocation required for breaches would interfere with the primary mandate of a custodian, but it would also negatively impact other organizations or public bodies involved with breach notification.

For example, if Eastern Health reported an average of 40 material breaches per fiscal year, there would be 40 incidences where notification and/or reporting would be required. If Eastern Health had an average of 170 breaches in total per fiscal year, and if mandatory breach notification and reporting for all breaches were implemented, there would be an increase in notification and reporting from 40 to 170, which would result in an increase of 425%. This increase would overwhelm an already heavily taxed resource. It is crucial for Eastern Health to maintain the effective response to material breaches that is already achieved with the current requirements for notification and reporting.

D.2. NOT REMOVING THE DOUBLE NEGATIVE WORDING REGARDING THE NOTIFICATION PROTOCOL

Eastern Health operates in the best interest of its clients to provide reasonable notification during these incidents. Ambiguity in the wording impedes the notification process. Not removing the double negative wording could lead to situations where there has been a delay in notification when

there should not have been, or it could lead to situations where notification should not have been delayed and it was. Both situations could adversely impact a client.

D.3. DETERMINING THAT NO FEES FOR RELEASE OF INFORMATION BE CHARGED

PHIA does not currently address the issue of custodians charging fees for the release of Information. In its current wording, the charging of fees is discretionary, which permits for variability with respect to not only what is charged but the amount charged.

Eastern Health processes approximately 25,000 requests for release of Information per year. The processing and printing of the requests is resource taxing. The committee should consider the financial impact to the regional health authority for all proposed enhancements.

E. SUMMARY

The *Personal Health Information Act* (PHIA) has proven to be very beneficial in aiding in the protection of Information. Improvements such as those referenced in this document will, once implemented, further enhance that protection and better enable custodians to execute their responsibilities with respect to protecting Information.

Eastern Health thanks the PHIA Review Committee for the opportunity to make this submission, which is based on our experiences with respect to PHIA. We are committed to continuously improving our compliance with privacy legislation.

APPENDIX A

Custodian

4.(1) In this Act, "custodian" means a person described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with the performance of the person's powers or duties or the work described in that paragraph:

(a) an authority;

(b) a board, council, committee, commission, corporation or agency established by an authority;

(c) a department created under the Executive Council Act , or a branch of the executive government of the province, when engaged in a function related to the delivery or administration of health care in the province;

(d) the minister, where the context so requires;

(e) a health care professional, when providing health care to an individual or performing a function necessarily related to the provision of health care to an individual;

(f) a health care provider;

(g) a person who operates

(i) a health care facility,

(ii) a licensed pharmacy as defined in the Pharmacy Act, 2012 ,

(iii) an ambulance service, or

(iv) a centre, program or service for community health or mental health, the primary purpose of which is the provision of health care by a health care professional or health care provider;

(h) the Provincial Public Health Laboratory;

(i) the Centre for Health Information;

(j) with respect to Memorial University of Newfoundland, the Faculty of Medicine, the School of Nursing, the School of Pharmacy and the School of Human Kinetics and Recreation;

(k) the Centre for Nursing Studies;

(l) the Western Regional School of Nursing;

(m) a person who, as a result of the bankruptcy or insolvency of a custodian, obtains complete custody or control of a record of personal health information, held by the custodian;

(n) a rights advisor under the Mental Health Care and Treatment Act ;

(o) the Workplace Health, Safety and Compensation Commission; and

(p) a person designated as a custodian in the regulations.

Personal health information

5. (1) In this Act, "personal health information" means identifying information in oral or recorded form about an individual that relates to

(a) the physical or mental health of the individual, including information respecting the individual's health care status and history and the health history of the individual's family;

(b) the provision of health care to the individual, including information respecting the person providing the health care;

(c) the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance;

(d) registration information;

(e) payments or eligibility for a health care program or service in respect of the individual, including eligibility for coverage under an insurance or payment arrangement with respect to health care;

(f) an individual's entitlement to benefits under or participation in a health care program or service;

(g) information about the individual that is collected in the course of, and is incidental to, the provision of a health care program or service or payment for a health care program or service;

(h) a drug as defined in the *Pharmacy Act, 2012* , a health care aid, device, product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care professional; or

(i) the identity of a person referred to in section 7.

(2) For the purpose of paragraph (1)(b), "information respecting the person providing health care" means, in relation to that person, the following information as applicable:

(a) the name, business title, address and telephone number;

(b) licence number; and

(c) profession, job classification and employment status.

(3) In addition to the matters referred to in paragraphs (1)(a) to (i), personal health information includes identifying information about an individual that is contained in a record that contains personal health information within the meaning of that subsection.

(4) Notwithstanding subsection (3), personal health information does not include identifying information contained in a record that is in the custody or under the control of a custodian where

(a) the identifying information contained in the record relates primarily to an employee or agent of the custodian; and

(b) the record is created or maintained primarily for a purpose other than the provision of health care or assistance in providing health care to the employee or agent.

(5) For the purpose of this section, "identifying information" means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or together with other information, to identify an individual.

Obligations of employees, etc.

14.(1) A custodian shall ensure that

(a) its employees, agents, contractors and volunteers; and

(b) where the custodian is an operator of a health care facility, those health care professionals who have the right to treat persons at a health care facility operated by the custodian,

take an oath or affirmation of confidentiality.

Security

15.(1) A custodian shall take steps that are reasonable in the circumstances to ensure that

(a) personal health information in its custody or control is protected against theft, loss and unauthorized access, use or disclosure;

(b) records containing personal health information in its custody or control are protected against unauthorized copying or modification; and

(c) records containing personal health information in its custody or control are retained, transferred and disposed of in a secure manner.

(2) For the purpose of paragraph (1)(c), "disposed of in a secure manner" in relation to the disposition of a record of personal health information does not include the destruction of a record unless the record is destroyed in such a manner that the reconstruction of the record is not reasonably foreseeable in the circumstances.

(3) Except as otherwise provided in subsections (6) and (7), a custodian that has custody or control of personal health information shall notify the individual who is the subject of the information at the first reasonable opportunity where the information is

(a) stolen;

(b) lost;

(c) disposed of, except as permitted by this Act or the regulations; or

(d) disclosed to or accessed by an unauthorized person.

(4) Where a custodian reasonably believes that there has been a material breach as defined in the regulations involving the unauthorized collection, use, or disclosure of personal health information, that custodian shall inform the commissioner of the breach.

(5) Notwithstanding a circumstance where, under subsection (7), notification of an individual by a custodian is not required, the commissioner may recommend that the custodian, at the first reasonable opportunity, notify the individual who is the subject of the information.

(6) Where a custodian is a researcher who has received personal health information from another custodian under section 44, he or she may not notify an individual who is the subject of the information that the information has been stolen, lost, disposed of in an unauthorized manner or disclosed to or accessed by an unauthorized person unless the custodian who provided the

information to the researcher first obtains the individual's consent to contact by the researcher and informs the researcher that the individual has given consent.

(7) Subsection (3) and subsection 20(3) do not apply where the custodian reasonably believes that the theft, loss, unauthorized disposition, or improper disclosure or access of personal health information will not have an adverse impact upon

(a) the provision of health care or other benefits to the individual who is the subject of the information; or

(b) the mental, physical, economic or social well-being of the individual who is the subject of the information.

(8) Notwithstanding subsection (1), a custodian that has custody or control of personal health information that is the subject of a request for access under subsection 53(1) or for correction under subsection 60(1) shall retain the information for as long as necessary to allow the individual to exhaust any recourse under this Act that he or she may have with respect to the request.

Investigative powers

69. (3) Except as otherwise provided under subsection (4), a custodian shall produce to the commissioner a copy of the information demanded under paragraph (1)(a) within 14 days of receipt of the demand, notwithstanding another Act or regulations or a privilege under the law of evidence.

Response of custodian

74.(1) Within 15 days after receiving a report of the commissioner that contains a recommendation under subsection 72(2), the custodian shall decide whether or not to comply with the recommendation in whole or in part and shall give written notice of his or her decision to the commissioner and to the complainant.

APPENDIX B

Material breach

5. The factors that are relevant to determining what constitutes a material breach for the purpose of subsection 15(4) of the Act include the following:

   (a) the sensitivity of the personal health information involved;

   (b) the number of people whose personal health information was involved;

   (c) whether the custodian reasonably believes that the personal health information involved has been or will be misused; and

   (d) whether the cause of the breach or the pattern of breaches indicates a systemic problem.