Questions and answers for custodians about the *Personal Health Information Privacy and Access Act* (PHIPAA)

This document provides answers to some frequently asked questions about the The *Personal Health Information Privacy and Access Act* (PHIPAA).

This document is intended to help custodians understand PHIPAA. It is not intended as legal advice.

Table of Contents

General

1. What is the purpose of the Act?

The Personal Health Information Privacy and Access Act (PHIPAA) provides a set of rules that protects the confidentiality of personal health information and the privacy of the individual to whom that information relates. At the same time, the Act ensures that information is available, as needed, to provide health services to those in need and to monitor, evaluate and improve the health system in New Brunswick. It applies to personal health information in the health system regardless of form, including but not limited to paper records, microfilm, X-ray film and electronic records.

The Act identifies a series of rights that individuals have in regard to their personal health information – for example, the right to consent to the collection, use and disclosure of their personal health information unless the Act provides otherwise, as well as the right to request the correction of their personal health information and the right to request access to their personal health information.

After identifying those rights, the Act establishes a legal framework for the handling of personal health information to ensure that individuals' rights are respected.

2. Why was a new Act required?

Health information is one of the most sensitive forms of personal information. It is used for a number of purposes including patient care; financial reimbursement; medical education; research; social services; quality assurance; risk management; public health regulation and surveillance; and health planning and policy development. In recognition of this fact, many jurisdictions across Canada have enacted, or are developing, legislation to protect the privacy, confidentiality and security of personal health information.

Since Jan. 1, 2004, organizations in New Brunswick that collect, use or disclose personal information, including personal health information in the course of "commercial activities" such as private physicians' offices, private health-care clinics and laboratories and pharmacies, have been subject to the federal Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA has been identified by health-sector stakeholders as especially problematic for the organizations that collect, use or disclose personal health information for health-care purposes since it was not developed with the special needs of health care in mind. Similarly, the former New Brunswick public sector privacy legislation did not address the specific requirements of health care. PHIPAA provides more detailed rules for managing personal health information while providing some additional flexibility in privacy practices for the health-care sector to better facilitate patient care.

3. Who must abide by the Act?

Custodians

PHIPAA applies generally to a group of stakeholders throughout the health system and government referred to as "custodians." The Act defines a custodian as an individual or organization that collects, maintains or uses personal health information for providing or assisting in the provision of health care or treatment; in the planning and management of the health-care system; or in the delivery of a government program or service. Examples of custodians named in the Act and its regulations include: the Department of Health; regional health authorities; WorkSafeNB; hospitals; health-care providers (for example, physicians, dentists, nurses, pharmacists); public bodies (including but not limited to government departments and Crown corporations); ambulance operators; and individuals or organizations known as information managers that manage personal health information on behalf of another custodian. The Act applies to any personal health information collected, used, stored, disclosed and maintained by custodians. Organizations and individuals wishing to confirm whether they are a custodian should consult the Act and regulations and/or their legal adviser.

Information managers

An information manager is a special type of custodian under the Act. An information manager is an individual or organization that processes, stores, retrieves, archives, disposes, de-identifies or otherwise transforms personal health information on behalf of the custodian. This includes, for example, any individual or organization that provides information management or information technology services for the custodian or an organization that provides records storage, archival or disposal services for the custodian with respect to personal health information.

Information managers are required to comply with the Act with respect to their handling of personal health information. In addition, an information manager will be required to enter into a formal written agreement with the custodian to whom the information management services are being provided which addresses the security and protection of the personal health information entrusted to them.

Agents

An agent is any individual or organization that acts for or on behalf of a custodian with respect to collecting, using, disclosing or maintaining personal health information. Examples of agents include:

- employees of the custodian such as a receptionists or assistants employed by a physician or other health-care provider;
- contract employees and volunteers; and
- organizations such as Clinidata and New Brunswick Emergency Medical Services Inc. that provide health care services on behalf of a custodian.

Agents will be required to comply with the Act and to sign a written agreement with the custodian to this effect.

4. What information will be covered by the Act?

PHIPAA applies to personal health information held by custodians, regardless of format. Personal health information is defined in part as identifying information about an individual pertaining to that person's mental or physical health, family history or health care history. This includes:

- genetic information;
- registration information, including the Medicare number of the individual;
- information about payments or eligibility for health care or health-care coverage;
- information pertaining to a donation by the individual of any body part or bodily substance;
- information derived from the testing of a body part or bodily substance of the individual; and
- information that identifies the individual's health-care provider or substitute decision maker.

All parts of the Act apply equally to personal health information regardless of form, including information that is oral, written or photographed. It applies to information recorded or stored in media such as paper, microfilm, X-rays and electronic records. Examples of personal health information include:

- a medical record held by a physician;
- a patient record held by a hospital;
- X-rays and images of an individual;
- registration information (Medicare number and other information such as an individual's name and date of birth) held by the Department of Health to register individuals for insured services; and
- records of prescriptions filled by a pharmacist.

5. Is it possible to collect, use and/or maintain personal health information and not be considered a custodian subject to the Act?

Yes. The Act defines certain situations whereby an individual or organization may collect, use or disclose personal health information and not be considered to be a custodian. The most notable exception applies to individuals or organizations that collect, maintain, or use personal health information for purposes other than providing or assisting in the provision of health care, treatment and the planning and management of the health-care system, or for delivering a government program or service. This includes, unless otherwise stated in the regulations, employers (both public and private), insurance companies, regulatory bodies of health-care providers, and licensed or registered health-care providers who do not provide health care. For example, life insurance companies collect personal health information for processing an application for insurance, and employers may collect personal health information as part of mandatory routine medical exams or drug testing as a condition of employment. In these instances, PHIPAA will not apply. The collection, use, and disclosure of personal health information may, however, be subject to other federal or provincial privacy legislation depending on the circumstances.

6. Can I collect and use the Medicare number?

The legislation introduces restrictions on the collection and use of the Medicare number, which is considered a type of personal health information. Henceforth, no person is entitled to require the production of, or collect or use an individual's Medicare number except a person who requires its production, collection or use to provide health care; to verify the individual's eligibility to participate in a health-care program or receive a health-care service; or for the payment and management of the health-care system. Individuals have a right to refuse to provide their Medicare number to any person not authorized by the Act to require that it be produced or to collect and use it. The legislation also provides that any person, who requests a Medicare number from an individual, must advise the individual of his or her authority to do so.

7. I am a health-care professional already covered by PIPEDA. Does the provincial legislation, PHIPAA, now replace the federal legislation, PIPEDA?

Since Jan. 1, 2004, organizations in New Brunswick that collect, use or disclose personal information, including personal health information in the course of "commercial activities" such as private physicians' offices, private health-care clinics and laboratories and pharmacies have been subject to the federal Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA has been identified by health-sector stakeholders as especially problematic for the organizations that collect, use or disclose personal health information for health-care purposes since it was not developed with the special needs of health care in mind. PHIPAA provides more detailed rules than PIPEDA and also provides some additional flexibility in privacy practices for the health sector.

With the introduction of PHIPAA, custodians engaged in commercial activities will continue to be bound by PIPEDA. However, they will now also be required to comply with PHIPAA with respect to the personal health information that they collect, use, disclose and maintain.

While there is generally more flexibility under PHIPAA with respect to the use and sharing of personal health information with other health-care practitioners, there are additional obligations imposed on custodians under the Act.

8. Our organization is a public body that collects, uses, and maintains personal health information. We have always been subject to privacy legislation in New Brunswick. What is changing for us?

Personal health information collected, used and disclosed by public health-care organizations such as hospitals, regional health authorities, the Department of Health and other government departments and agencies was previously subject to the former provincial privacy legislation, the Protection of Personal Information Act (POPIA). The former provincial Right to Information Act also applied with respect to providing access to individuals' personal information. These two Acts are replaced by PHIPAA and the new Right to Information and Protection of Privacy Act (RTIPAA). Organizations that are public bodies may need to comply with one or both Acts, depending on the nature of the personal information they collect, use or disclose. To the extent that a public body collects, uses, or discloses personal health information or maintains personal health information within its custody or control for the purpose of providing or assisting in the provision of health-care or treatment, the planning and management of the health care system, or for delivering a government program or service, it will be considered a custodian and PHIPAA will apply to that information. This includes government departments or agencies that are not health-care facilities but that may process or handle personal health information in administering their programs or services such as the Department of Social Development or Service New Brunswick.

RTIPPA will apply to all records containing personal information in the organization's custody or control that is not considered to be personal health information. Public body custodians must understand the nature of the information that they collect and maintain to determine whether they will be a custodian under PHIPAA and therefore need to comply with both Acts.

9. What are the responsibilities of a custodian under the Act?

PHIPAA identifies several rules that custodians must follow in the collection, use, disclosure, secure destruction, and protection of personal health information. In addition to complying with specific obligations that may apply depending on the circumstances under which personal health information is being used or disclosed, every custodian must:

- obtain consent to collect, use or disclose personal health information except in a limited number of situations, such as in the case of a health emergency. (Note that consent may either be express or implied. For the specific purposes of providing health services to an individual, the Act recognizes that consent is implied for sharing personal health information within the "circle of care" for the provision of health services to individuals). For more information on consent, refer to Question 11;
- only collect, use and disclose the minimum amount of information necessary to provide the service or benefit being offered;
- inform the individual about the intended use and disclosure of the information and ensure that there are policies in place to ensure information is only used and disclosed in accordance with the Act;
- designate a person to respond to inquiries and complaints and to ensure compliance with the Act;
- establish effective procedures for responding to individuals' requests for access to, or correction of personal health information in compliance with the Act;
- establish and implement appropriate information practices, including policies and practices, that will protect the integrity, confidentiality, security and accuracy of personal health information. This includes, but is not limited to, the following specific policies and procedures:
    - completion of a privacy impact assessment for new or changed collections, uses and disclosures of personal health information by custodians that are public bodies;
    - security policies outlining administrative, technical and physical safeguards for protecting personal health information, and procedures for recording and managing security breaches; and
    - a written policy for the retention, archival storage, access and secure destruction of personal health information.
- where outside service providers are engaged to process personal health information on the custodian's behalf, follow specific rules to ensure that personal health information is appropriately protected while it is processed while in

the custody and control of the other organization. This includes entering into formal written agreements with these information managers for the protection of personal health information and acknowledging that, as a custodian, they are required to comply with the provisions of the Act.
- implementing controls to ensure that agents (such as employees, volunteers and contractors) who collect, use or disclosure personal health information on the custodian's behalf comply with the Act.
- implement procedures to assess the potential impact of a breach of personal health information and to comply with the requirements under the Act for notifying individuals as well as the Access to Information and Privacy Commissioner.

10. What rights are granted to individuals under the Act?

PHIPAA identifies a number of rights that individuals have in regard to their personal health information including the right to:

- be informed about the purpose for the collection and the anticipated uses and disclosures of his or her personal health information;
- withhold or withdraw consent for the collection, use and disclosure of his or her personal health information, except in specific circumstances outlined in the Act;
- designate another person to make decisions about his or her personal health information;
- request to examine or receive a copy of his or her personal health information (providing such access may be subject to the individual paying a fee);
- request correction of his or her personal health information once he or she has examined it;
- refuse to provide his or her Medicare number to any person or organization that collects the information as identification for a non-health service;
- be informed if his or her personal health information has been lost, stolen, or otherwise inappropriately destroyed, disclosed to or accessed by an unauthorized person where it is reasonable to conclude that this could identify or otherwise harm the individual;
- make a complaint to the Access to Information and Privacy Commissioner about:
    - a custodian's decision with respect to the individual's request to access or correct his or her record; or
    - a custodian's information practices if the individual believes that the custodian has collected, used or disclosed his or her personal health information contrary to the Act or failed to protect his or her personal health information contrary to the Act or failed to protect his or her personal health information; and
- appeal or refer a matter to court.

Collection, use, disclosure, and secure destruction

11. What obligations does PHIPAA place on custodians' collection, use and disclosure of personal health information?

Disclosing personal health information is a sensitive issue. It is often essential to facilitate the provision of a health service. For example, a physician must disclose some personal health information to refer a patient to a specialist or to arrange for needed surgery. Yet disclosing personal health information also means revealing very private information about an individual to another person. Because this affects the privacy of the individual, the Act creates strict rules for using and disclosing personal health information while balancing the legitimate needs of health-care custodians to share information for patient care and treatment and the appropriate management of the health care system. In particular:

- a custodian must ensure that personal health information is only collected, used by or disclosed to those employees or agents who need to know the information to carry out the original purpose for which the information was collected;
- custodians must ensure that every collection, use or disclosure of information is limited to the minimum amount of information necessary to accomplish the original purpose for which the information was collected. For example, for

the Department of Health to issue payment to a physician for a service provided to a patient, the department will only receive the minimum information required to know what to pay. The department will not have access to any other information contained in the records of the physician about that service;

- information can only be collected, used or disclosed by a custodian with the consent of the individual or for purposes permitted in the Act (refer to Sections 11.1 and 11.2).
- when it is no longer required, personal health information must be destroyed in a secure manner in order to protect individuals' privacy.

11. 1 Implied knowledgeable consent and the circle of care

For the specific purposes of providing health care to an individual, a patient-centred, "circle of care" is created where information is appropriately shared. PHIPAA permits health-care providers to collect or use the individual's personal health information or to disclose that information to another custodian or person within this circle of care for providing health care to that individual only with that person's continuing implied knowledgeable consent.

For implied knowledgeable consent to exist, individuals must first have been informed about the purpose of the collection, use and disclosure and must be aware that they have a choice to give, withhold or withdraw their consent to the collection, use or disclosure of their personal health information in accordance with the Act. Where a custodian posts or makes readily available a notice describing the purpose of the collection, use and disclosure or provides the individual with such a notice they will be considered to have been appropriately informed.

These provisions ensure that health providers who need to know pertinent information about individuals to care for and treat them are entitled to continue to use that information for those purposes as long as they have the individual's continuing implied knowledgeable consent. For example, the Act permits the sharing of an individual's personal health information between a specialist and his or her family physician when he or she is being treated in hospital as long as he or she has been appropriately informed about how his or her information will be shared and understand his or her rights with respect to providing or withdrawing consent.

The Act also creates strong "walls" of consent and security around the circle of care. For example, if an individual reveals personal information to hospital staff as part of the admittance procedure, consent for the use and disclose of the individual's personal health information will be considered to be implied for the purposes of the visit to the hospital (as long as it is reasonable to assume that the individual knows the purpose of the collection and how the information will be used and disclosed for the provision of health care). Any use or disclosure beyond that requires express consent or must be based on an exception identified in the Act.

Custodians must also educate their agents on these requirements and require that they comply.

11.2 Disclosure without consent in limited circumstances only

The Act provides for other circumstances where personal health information may be disclosed without consent. For example, if a custodian receives a subpoena to disclose personal health information to a court, consent of the individual is not required – the custodian must comply. Other instances where personal health information may be disclosed without consent include making information available for an information network or a registry (such as a cancer registry) where the information is to be used for facilitating or improving the provision of health care or the monitoring and evaluation of a health care program or the health-care system; obtaining payment for health care services; for public health reasons; and other reasons which are detailed within the Act.

For other purposes not provided for in the Act or otherwise required by law, the Act clearly states that express consent of the individual must be obtained.

12. What new obligations does the Act place on custodians that engage third-party service providers to manage personal health information on their behalf?

A custodian may provide personal health information to an information manager for processing, storing or destroying that information or for providing the custodian with information management or information technology services. An example of an information manager is an organization that provides records storage, archival or disposal services for a physician's office or hospital. Custodians who engage information managers to process information on their behalf must follow specific rules to ensure that personal health information is appropriately protected while it is processed at the other organization. A custodian must:

- Require the information manager to sign a written agreement with the custodian that:
  - describes the services to be provided by the information manager;
  - outlines how the personal health information will be protected against risks such as unauthorized access to or use or disclosure, unsecure destruction or alteration of the information;
  - requires the information manager comply with the Act and regulations.
- Ensure that information managers do not store personal health information outside of Canada unless the information manager is providing maintenance and technical support for personal health information systems or unless otherwise provided for in the Act.

13. What rules does the Act outline for a custodian that owns an information network or collects, uses or discloses personal health information in the context of an information network?

The health-care system uses information technology to link the computer systems of two or more custodians to permit personal health information to be shared. This is referred to as an information network. The purpose of such a network is to facilitate patient care and to improve the planning and management of the health-care system. As an example, the Department of Health is the custodian of the Electronic Health Record, which has been designated as an information network.

Personal health information in an information network and will be protected in a number of ways. The following facts are important to know:

- the Minister of Health must formally designate a health information system as an information network under PHIPAA.
- a person seeking to designate any existing or proposed technology as an information network will apply to the Chief Privacy Officer of the Department of Health by providing the following information:
  - the purpose of the information network for which personal health information may be collected and used;
  - the type or nature of personal health information to be contained in the information network, and the source of the personal health information;
  - the custodian to be named as owner of the information network;
  - the employee(s) of the owner proposed as administrator of the information network;
  - the purposes for which personal health information may be collected, used and disclosed;
  - roles-based analysis of individuals who will collect, use or disclose personal health information through the information network to ensure that only those individuals who need to know the information to accomplish the stated health-care purpose are provided access to the network;
  - whom personal health information may be collected into the information network, including whether personal health information will be collected directly or indirectly from the individual;
  - except in the case of disclosure for a planning or research purpose, identify to whom personal health information contained in the information network may be disclosed; and
  - the limits or conditions, if any, on the collection, storage, use or disclosure of personal health information

contained in or disclosed from a information network, including the types of consent directives that may be entered into the information system.

- As information networks are designated under the legislation, the above information will be posted to the Department of Health's website. These measures are designed to increase transparency to the public in accordance with custodians' obligations under PHIPAA.
- Sharing of information within an information network will only be permitted among health-care custodians within the circle of care and only for the specific purposes outlined in the Act. In all other cases, the consent of the individual will be required prior to disclosure of personal health information.

13.1 Consent directives within an information network

- An individual may register a consent directive within an information network to prevent access to personal health information by a user who would normally be provided access to the record for the identified purposes of the information network.
- Applications for consent directives must be submitted in writing to the administrator of the information network. They are effective once registered in the information network. A consent directive may only be changed or revoked with written notice to the owner. It is important to note that a consent directive will be applied to the entire content of an individual's record. For administrative reasons, a consent directive may not be applied only to part's of an individual's record within an information network.

14. Can anything override a person's expressed instructions not to disclose personal health information?

The Act provides that custodians are entitled to assume that they have the patient's implied knowledgeable consent to collect, use and disclose the individual's information for providing health care or assisting in the provision of care to the individual once they have clearly informed the individual of the purpose for the collection, use and disclosure; and once the individual is aware of their right to withhold or withdraw consent. Implied and knowledgeable consent will be considered to exist in these circumstances unless the custodian is aware that the individual has expressly withheld or withdrawn the consent. An individual may expressly instruct the custodian not to make the disclosure or use by issuing a consent directive (as described above).

However, consent directives are of no effect against disclosures that are required by law or otherwise authorized under PHIPAA and may be overridden in certain circumstances. For example, the Act provides that a health-information custodian may disclose personal health information about an individual, without consent, if the custodian believes on reasonable grounds that the disclosure is necessary for eliminating or reducing a significant risk of serious bodily harm to a person. A consent directive will not apply in these specific circumstances. A health-care provider may override an individual's consent directive if, in the judgment of the health-care provider, it is necessary to provide health care to the individual and the individual is not capable of providing consent.

15. Can personal health information be disclosed for research?

Personal health information can be an indispensable resource when conducting research to prevent disease or find new cures or treatments. The public benefits from reliable, ethical research can be significant; however, it cannot happen without proper safeguards to protect personal privacy. The Act sets out rules under which custodians can disclose personal health information for research. In particular, it requires all research proposals to be reviewed and approved by a recognized research review body. The Act provides for several criteria that must be assessed by the research review body in evaluating a research proposal including: obtaining consent of the individual(s) prior to the use and disclosure of his / her / their information unless it is impractical to do so; assessing whether disclosing de-identified information will serve the same research purpose as disclosing

identifiable information; and assessing whether only the minimum amount of identifiable personal health information required for the research project is disclosed.

The Act also requires that the custodian, as a condition of being granted approval for the research project and the related disclosure of personal health information, enter into an agreement with the third party researcher in which the third party agrees:

- not to publish the personal health information requested in a form that could reasonably be expected to identify the individuals to whom the information relates;
- to use the personal health information requested solely for the purposes of the approved research project; and
- to ensure that reasonable safeguards and procedures are in place to protect the information and to securely destroy it once it is no longer required.

Providing access to records; correcting records

16. What obligations does a custodian have as it related to providing individuals access to their own personal health information?

Individuals are entitled to request access to their personal health information that they believe to be in the possession of a custodian by making a request in writing. The Act provides a number of rules that custodians must follow in this regard:

16.1 General obligations related to providing access

Q: What procedures must I have in place regarding providing access to individuals?

A custodian must:

- establish procedures and practices for enabling and responding to individuals' requests for access to, or correction of their personal health information;
- offer assistance to the person who made the request to reformulate it if it does not contain sufficient detail to permit the custodian to identify and locate the record;
- respond to a request no later than 30 days after receiving it, unless there are specific reasons for extending the time needed for responding to the request (such as when there is an extremely large volume of records to be searched);
- transfer the request to another custodian if the requested records are maintained by or were first collected by the other custodian within 10 days. Inform the individual that his or her request has been transferred;
- make information available for examination or provide a copy if the individual requests it (which may be subject to the individual paying a fee, as outlined in the Act and regulations);
- inform the individual in writing if the information does not exist or cannot be found;
- inform the individual in writing if the request is refused, in whole or in part, for a specified reason. Where access is denied, the custodian must provide the reasons for denying access. Exceptions may include, for example, information that contains references to other individuals; or information that is subject to solicitor-client or litigation privilege; and
- inform the individual of right to file a complaint with the Access to Information and Privacy Commissioner or refer the matter to court if the individual does not agree with the custodian's decision.

16.2 Official Language considerations

Q: Am I obligated to have a record translated for an individual to accommodate their language preference?

A custodian is not obligated to have a record translated for an individual. However, a custodian subject to the Official

Languages Act in New Brunswick must provide access to a physician or other health-care provider who can help individuals in interpreting their record in the official language of their choice if they request it. If the health-care provider helping the individual is unilingual and unable to understand the record sufficiently, the custodian must translate the relevant portions of the record for the interpreter first.

16.3 Exceptions to access

Q: What exactly are the constraints on disclosure related to matters involving litigation?

With respect to matters involving litigation, such as situations where a medical examination was conducted in the course of litigation or a similar claim, the Act provides for a number of exceptions that may apply, including situations where:

- the information was compiled principally in anticipation of, or for use in, a civil, criminal or quasi-judicial proceeding to which the custodian is or may be a party or is protected by privilege;
- the information is protected by privilege;
- another Act of the Legislative Assembly of New Brunswick or the Parliament of Canada or a court order prohibits disclosure of the personal health information to the individual; and
- the personal health information was collected for purposes of an investigation conducted pursuant to an Act of the Legislative Assembly of New Brunswick.

There may be other exceptions that apply, depending on the facts of the particular situation. The Act should be consulted for a comprehensive list of exceptions available. It should also be noted that, wherever possible, a custodian is required to sever the personal health information that cannot be examined or copied (due to the application of a particular exception[s]) and permit access to or a copy of the remainder of the record.

16.4 Third-party requests

Q: While there is a specific right of a patient to examine or copy records, is there is a specific right to have information transferred to another party at the request of the individual?

The Act does not grant particular rights to individuals to have their information transferred to another party. However, an individual who wishes to have their personal health information provided to another individual may do so by consenting in writing. A custodian receiving such a request has certain duties under the Act to ensure that the disclosure is made only to the person who has been authorized to receive the information. To this end, custodians should ensure that appropriate precautions are taken before releasing information such as:

- ensuring that the individual's consent to release the information to a third party is received in writing, dated and signed and that it is the original document (as opposed to a copy); and
- taking steps to ensure the validity of the request such as:
    - visually confirming the identity of the individual; and
    - contacting the individual to confirm the validity of his or her request, and, if necessary, to confirm the intended scope if the consent document is worded in a broad manner. In regard to the latter circumstance, an example would be legal counsel who represents a client in respect of a soft tissue injury in a motor vehicle accident. While certain portions of a medical record would be relevant to the legal action, the patient may not wish his or her legal counsel to see his or her entire medical history.

17. Is there any format for appropriate "correction" of a record? Is there anything in the Act to preclude a custodian correcting a record without a specific request from a patient/client?

Individuals may request corrections to their records by making a written request of the custodian. If the custodian agrees with and approves the request, the custodian must make the corrections involved. The Act requires custodians to ensure that requested corrections to records are made such that the correction is either incorporated directly within the record or is cross-referenced from within the original documentation. A new version of the record marked as such will suffice for this purpose. The new version would not be required to reference the original information if the change has been incorporated within it. Custodians are not required to keep the original record where a change has been requested and agreed upon. However, as a best practice, custodians should keep records of all requests for correction of the original record.

Similarly, if a custodian refuses to make a correction that an individual has requested the custodian if required to permit the individual to file a concise statement of disagreement stating the correction requested and the reason for the correction. The custodian must add the statement of disagreement to the record in a manner that it will be read with and form part of the record or be adequately cross-referenced to it.

If a custodian makes a correction or adds a statement of disagreement, the custodian must, when practicable, notify any other custodian or person to whom the personal health information has been disclosed about the correction or statement of disagreement. The other custodian is required to make the correction or add the statement of disagreement, if applicable, to any record of the personal health information that the custodian maintains.

Nothing in the Act precludes a custodian correcting a record without a specific request from a patient/client if the change is being made to improve the accuracy or completeness of the record in the normal course of the custodian's operations. In fact, the Act requires all custodians to take reasonable steps before using or disclosing personal health information to ensure that the information is accurate, up-to-date and complete. If a custodian becomes aware of an inaccuracy in a record, that custodian would be obligated to correct it.

The Act requires custodians to correct any record of the individual's personal health information that they maintain. Therefore, if the personal health information is maintained in records kept in more than one format, such as paper and electronic, custodians must ensure that the change in incorporated within all formats of the record, including the original and copies of the record.

18. Could a custodian charge an individual for assistance with interpreting the record?

PHIPAA provides that a custodian shall permit an individual to examine a record free of charge. However, the custodian may require an individual to pay to the custodian a fair and reasonable fee for search, preparation, copying and delivery services.

Where the Act and its regulations are silent on specific aspects of fees that may be charged, such as in the case of assisting an individual in interpreting the record, there are a number of factors that may be considered, including a physician or other health-care practitioner's professional guidelines or code of ethics; whether the intended fee is fair and reasonable; and whether all or part of a fee should be waived in cases where charging a fee might impose an unreasonable financial hardship on the applicant. In the case of providing assistance with interpreting a record, a custodian may also wish to consider whether it would be reasonable to conclude that such activity is part of examining the record or is an entirely separate activity.

Retention and secure destruction

19. While the Act contains an obligation to maintain security and privacy of records, is there an obligation to retain them for any specific period, or otherwise avoid their destruction?

The Act does not define a specific period for which records must be retained by a custodian, nor does it provide guidance on particular types or categories of records that must be retained indefinitely.

The Act requires, however, every custodian to establish and comply with a written policy for the retention, archival storage and access and secure destruction of personal health information. The Act requires that the policy meet any legal requirements applicable to the custodian and that it protect the privacy of the individual to whom the information relates.

A custodian's retention policy for various categories of personal health information will depend upon a number of factors including specific legal, organizational, and stakeholder requirements. Specific points of consideration include:

- generally, health-care legislation in New Brunswick prescribes certain minimum, not maximum, periods of retention for patient records;
- a longer period of retention may be appropriate, depending on the needs of the organization and its stakeholders;
- retaining information for longer than the legal requirement has the potential to increase potential risks associated with unauthorized access to, or use of the information; this could compromise the privacy of individuals; and
- information should generally be retained for a reasonable period sufficient to allow the individual to whom the information relates an opportunity to obtain access to it.

20. Does the Act's reference to the destruction of records refer only to the original or to all of the information contained therein? What is the impact on destruction of the original and retention of a copy by other means?

Generally, records management best practices require destruction of all copies and all versions of a particular record that has been authorized for destruction, including back-up copies and copies stored in offsite storage locations. Also, records should be managed according to their content, regardless of media or storage location. For example, if the original record is kept in a paper file and copies are retained electronically, both the original and the copies would be destroyed when the custodian's record retention schedule requires secure destruction. A good information management practice is to maintain as few copies and storage locations for the same records as possible. The retention of unmanaged or unnecessary copies of records may pose an increased privacy risk to individuals.

The Act requires a custodian who destroys personal health information to keep a record of the individual whose personal health information is destroyed, a summary of the contents of the record, the time period to which the information relates, the method of destruction and the name of the person responsible for supervising the secure destruction. The custodian is also responsible to ensure that the destruction of all personal health documents in his custody and control is completed in a manner that assures the confidentiality of the documents at all steps of their disposal.

21. What is meant by keeping a "summary of the contents" of the records destroyed?

Consistent with good information and records management practices, the Act requires a custodian to keep a summary of the content of the records destroyed according to its records retention policy. This ensures that, although the physical contents of the record are destroyed, a record of its existence is maintained in perpetuity. If an individual has requested access to a record that has been destroyed, a custodian should be able to confirm certain basic information about the records destroyed and demonstrate that records were destroyed in accordance with a consistent retention and destruction policy. A record of destruction providing a summary of the contents of the records destroyed might be kept in a table format as outlined in the following example:

Name of individual	Summary of contents	Time period	Date and method of destruction	Destruction supervised by: (name of person)
Jane Doe	Describe the nature of the records – eg "Medical examination records" or "dental records"	1982-1990	April 1, 2010 Secure shredding	John X

Other topics

22. Am I permitted to transfer files or store records containing personal health information outside the province, and would I need to notify the individuals whose records are transferred?

A custodian is permitted to disclose personal health information outside the province without the express consent of the patient as may be necessary to provide health-care to an individual. For example, patients are often referred to out-of-province physicians for treatment; or laboratory samples or radiological images are referred for assessment. Likewise, disclosures may be made for purposes related to administration of the health-care system, including billing for publicly funded health-care services.

Out-of-province disclosures may also be made to an information manager, which is an entity that processes, stores, retrieves, archives or disposes of personal health information on behalf of the custodian. Such arrangements must include data sharing agreements that meet the requirements specified in the Act.

A custodian is not permitted to store personal health information outside of Canada unless the Act provides otherwise.

23. What happens to client or patient records containing personal health information when the custodian dies?

In the event that a custodian dies, the custodian's personal representative assumes the duties and powers of a custodian under the Act until the custody and control of the personal health information passes to another person who is legally

authorized to hold the record. The custodian's personal representative generally has the following options with respect to the maintenance of the records containing personal health information:

- continuing to assume all of the duties and powers of a custodian under the Act, including duties associated with maintaining and providing access as requested to individual records of personal health information;
- transferring the records to another custodian, in which case the Act requires that clients or patients of the deceased custodian be notified about the personal health information held by the new custodian, how long it will be retained, and where they may make a written request for access to the personal health information; or
- transferring the records to an information manager such as an outside records management organization that can appropriately archive and maintain the records on his/her behalf. As discussed, the Act imposes certain restrictions and requirements that must be in place when dealing with information managers.

24. What is a privacy impact assessment, and will I need to do one?

A privacy impact assessment is a systematic examination of all collections, uses and disclosures of personal health information by the organization and its agents, that identifies risks and mitigation strategies to reduce those risks. The Act requires that all public bodies perform a privacy impact assessment on new or modified initiatives that involve the collection, use or disclosure of personal health information. Subject to limited exceptions, most government departments, offices, boards, Crown corporations or commissions, municipalities, school districts, universities, and community colleges are considered to be public bodies. The Right to Information Act should be consulted for a more detailed definition of what is considered to be a public body.

Health-care providers in private practice will not be required by law to conduct a privacy impact assessment, but, as a best practice, they may wish to do so.

25. What is a privacy breach? If a privacy breach occurs, what are my obligations as a custodian?

A privacy breach occurs any time that personal information is stolen, lost, disposed of, except as permitted by this Act, or disclosed to or accessed by an unauthorized person.

If any of these situations occur, there may be a requirement to notify the individual to whom the information relates and the Access to Information and Privacy Commissioner. In determining whether notification will be required, a custodian must consider whether it is reasonable to conclude:

- that the breach may have an adverse impact on the provision of health care or other benefits to the individual to whom the information relates or on the individual's mental, physical, economic or social well-being, or
- that the breach may lead to the identification of the individual to whom the information relates.

Where notification is required, the custodian must notify the individual and the Access to Information and Privacy Commissioner at the earliest opportunity by providing specific information outlined in the Act and regulations, including:

- the name of the custodian;
- the name of a contact person for the custodian and their contact information;
- the nature of the breach;
- the date the breach occurred and the date it came to the attention of the custodian;
- the cause of the breach; and
- the location of the breach.

Custodians should implement procedures to assess the potential impact of a breach of personal health information and to comply with the requirements under the act for notifying individuals and the Access to Information and Privacy Commissioner. Agents and information managers of the custodian should be required to immediately notify the custodian in the event of a breach.

26. What is the role of the Access to Information and Privacy Commissioner?

The Access to Information and Privacy Commissioner has several duties and powers under the Act, including:

- powers to investigate complaints brought forward by individuals regarding a custodian's response to a request for access to or correction of a record of personal health information;
- powers to investigate complaints regarding a custodian's treatment of personal health information in accordance with the Act;
- monitoring how the Act is administered and making recommendations where the Commissioner deems appropriate;
- conducting investigations to monitor compliance with Act, including investigating breaches of personal health information;
- reviewing, at his or her discretion, the privacy impact assessments that have been conducted by a custodian that is a public body;
- informing and educating the public about the Act;
- promoting best practices in privacy protection and access to health information as well as and providing advice to custodians; and
- reviewing matters referred to the Commissioner by the provincial government.