An overview of the *Personal Health Information Privacy and Access Act (PHIPAA)*

with comparison to the

Personal Information Protection and Electronic Documents Act (PIPEDA)

By:
DEIRDRE L. WADE, Q.C.,
and
COLIN A. FRASER

BARRY SPALDING
Suite 710, 55 Union St.,
P.O. Box 6010, RPO Brunswick Square,
Saint John, New Brunswick.
E2L 4R5

506-633-4226

May 17, 2010

Table of Contents

Preamble

This document is organized in three parts.

Part one provides a general introduction;

Part two provides an overview of the application of PHIPAA to assist custodians in understanding the obligations and responsibilities imposed upon them by the Act and the rights of individuals in connection with their PHI; and

Part three provides a comparison of key provisions of PHIPAA and PIPEDA for those health-care professionals, businesses and organizations that must comply with both acts.

Part 1: Introduction

Background

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. Self-regulating health professions governing physicians, nurses, dentists and physiotherapists have consistently imposed on their members an obligation to maintain the privacy and confidentiality of personal health information (PHI) to which the health-care professional may have access or acquire access.

Recent advances in technology are making PHI much more widely accessible and able to be shared among those in the health-care system for the benefit of the patient and health care generally. While there are benefits and risks with respect to this increased accessibility, the maintenance of privacy and confidentiality must remain as fundamental principles.

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.

In recognition of these facts, many jurisdictions across Canada have enacted, or are developing, legislation to protect the privacy, confidentiality and security of PHI.

The New Brunswick's Personal Health Information Privacy and Access Act (PHIPAA) applies to PHI that has been or will be collected, used or disclosed by a custodian or that is in the custody or control of a custodian. A custodian is any individual or organization that collects, maintains or uses PHI for providing or assisting in providing health care or treatment; planning and managing the health-care system; or delivering a government program or service.

Since Jan. 1, 2004, organizations such as private physicians' offices, private health-care clinics and laboratories and pharmacies in New Brunswick that collect, use or disclose personal information, including PHI in the course of "commercial activities," have been subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). The organizations that are currently subject to PIPEDA, will be subject to both PIPEDA and PHIPAA to the extent that they collect, use or disclose PHI in the provision of health care or treatment and are considered to be custodians under PHIPAA.

Purpose

This document is intended to be a general reference guide; it is an overview document only. For specific questions and/or legal advice and interpretation, custodians should consult PIPEDA (as applicable), PHIPAA and the regulations under both Acts as well as their legal advisers. In some cases, more specific questions can and should be directed to the regulators of the various health-care professions within the province.

Part 2: Overview of PHIPAA for custodians

A. Interpretation, purposes and application

This section is intended to provide a detailed overview and summary of PHIPAA for custodians. Custodians who are already subject to PIPEDA may wish to first refer to Part 3 of this paper to identify the key areas where PHIPAA will affect their information practices.

Purposes of PHIPAA

The *Personal Health Information Privacy and Access Act* (PHIPPA) provides a set of rules that protects the confidentiality of PHI 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.

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

The Act also provides for an independent review and resolution of complaints made in respect to PHI and provides effective remedies for contravention of the Act.

Application of PHIPAA

PHIPAA applies to PHI that is collected, used or disclosed by a custodian or that is in the custody or control of a custodian. Likewise, PHIPAA applies to any PHI collected before the proclamation of PHIPAA, and that is described in the regulations. It applies to PHI in the health system regardless of form, including but not limited to paper records, microfilm, X-ray film and electronic records.

Exceptions to the Application of PHIPAA

PHIPAA does not apply to:

- anonymous or statistical information that does not, either by itself or when combined with other information available to the holder of that information, permit individuals to be identified;
- an individual's PHI if 100 years have passed since the record containing the information was created or 50 years have passed since the death of the individual;
- an individual or organization that collects, maintains or uses PHI for purposes other than health care or treatment and the planning and management of the health care system, including:
  - employers;
  - insurance companies;
  - regulatory bodies of health-care providers;
  - licensed or registered health-care providers that do not provide health care; or
  - any other individual or organization that may be exempted by regulation;

- information in a court record, such as a record of support services provided to a judge or court official;
- PHIPAA is not intended to affect the law of evidence. PHIPAA does not restrict information that is otherwise available by law to a party to a legal proceeding; does not affect any information that would disclose privileged communications; and does not affect the power of a court or tribunal to compel a witness to testify or to compel the production of documents.
- PHIPAA is not intended to interfere with the activities of a body with statutory responsibility for the discipline of health care providers.

Custodians should consult the Act and regulations for more information on instances where PHIPAA may not apply.

Application of other legislation

PHIPAA does not prohibit the transfer, storage or disposition of a record in accordance with any other Act of the Legislature of New Brunswick or the Parliament of Canada.

In any circumstance where PHIPAA conflicts with the provisions of any other Act of the Legislature of New Brunswick, PHIPAA will prevail or govern. A conflict will not exist, however, unless it is impossible to comply with both PHIPAA and the other Act of the Legislature of New Brunswick.

There are specific rules in connection with PHI contained in records created or information held by persons for the purposes of the *Family Services Act*. *The Mental Health Act* prevails over PHIPAA.

The *Right to Information and Protection of Privacy Act* may apply to personal information maintained by a custodian that is not personal health information. This Act does not apply to PHI in the custody or under the control of a custodian unless PHIPAA states that it does. The specific provisions of the *Right to Information and Protection of Privacy Act* should be reviewed and considered in these instances.

Definitions

Listed below are definitions for several key terms defined in PHIPAA that are essential to a comprehensive understanding of the application of the legislation.

Personal Health Information (PHI)

PHI is defined as identifying information about an individual 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 if the information:

- relates to an individual's physical or mental health, family history or health-care history, including genetic information about the individual;
- is the individual's registration information, including the Medicare number of an individual;
- relates to the provision of health care to an individual;
- relates to information about payments or eligibility for health care in respect of an individual, or eligibility for coverage for health care in respect of an individual;
- relates to the donation by an individual of any body part or bodily substance of the individual or is derived from the testing or examination of any body part or bodily substance;
- identifies an individual's substitute decision maker; and
- identifies an individual's health-care provider.

Examples of PHI include:

- a medical record held by a physician, physiotherapist, dentist, chiropractor, or other health-care practitioner;
- 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.

What is health care?

Health care is defined as any observation, examination, assessment, care, service or procedure that is carried out or provided for a health-related purpose and:

- to diagnose, treat or maintain an individual's physical or mental condition;
- to prevent disease or injury or to promote health;
- as part of rehabilitative or palliative care.

It includes:

- the compounding of a drug, for the use of an individual, pursuant to a prescription;
- the dispensing or selling of a drug, a device, equipment or any other item to an individual, or the use of an individual pursuant to a prescription; and
- any health-care service prescribed by regulation.

What is a custodian?

PHIPAA defines a custodian as an individual or organization that collects, maintains or uses PHI for the purposes of providing or assisting in the provision of health care or treatment or the planning and management of the health-care system or delivering a government program or service and includes:

- Public bodies – defined in the *Right to Information and Protection of Privacy Act*;
- Health-care providers (for example, physicians, dentists, nurses, pharmacists);
- the Minister of Health;
- Ambulance New Brunswick Inc.;
- The New Brunswick Health Council;
- Facilicorp NB Ltd.;
- the regional health authorities;
- WorkSafe NB;
- Canadian Blood Services;
- Information managers (defined below);
- researchers conducting a research project approved in accordance with PHIPAA;
- health-care facilities (public or private medical clinics, hospitals, pharmacies, community health centres and other facilities in which health care is provided and that may be designated in the regulations.)
- a laboratory or specimen collection centre;
- nursing homes and operators; and
- any person designated in the regulations as a custodian.

Who is a health-care provider?

A health-care provider is defined as a person who is registered or licensed to provide health care under an Act of the Legislature of New Brunswick and who is a member of a class of persons designated as health-care providers in the regulations. Examples include but are not limited to physicians, nurses, physiotherapists, opticians, dentists and chiropractors.

What is an information manager?

An information manager is defined as an individual or organization that on behalf of a custodian processes, stores, retrieves archives or disposes of PHI, de-identifies or otherwise transforms PHI, or provides information management or information technology services. 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 PHI.

Information managers are required to comply with the Act with respect to their handling of PHI. 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 that addresses the security and protection of the PHI entrusted to them.

Who is an agent?

An agent is defined in relation to a custodian. An agent is an individual or organization that acts for or on behalf of the custodian in respect of PHI for the purposes of the custodian and not for the agent's purposes, whether or not employed by the custodian or being remunerated.

Examples of individuals and organizations that may be considered agents to the extent that they collect, use, disclose or retain personal health information on behalf of the custodian include:

- employees of the custodian such as receptionists or assistants employed by a physician or other health-care provider;
- contractors 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 by the Act to sign a written agreement with the custodian agreeing to comply with the Act if the custodian retains the services of an agent to act on behalf of the custodian for the collection, use, disclosure or retention of PHI.

B. Access to personal health information

An individual's right to examine or copy PHI

An individual has a right on request to examine or receive a copy of his or her PHI maintained by any custodian that the individual believes has custody and control of the individual's PHI. PHIPAA contemplates both informal oral requests to access PHI and formal written requests to access PHI. A request must contain sufficient detail to permit the custodian to identify and locate the record with reasonable efforts.

A custodian must respond to a request no later than 30 days after receiving the request unless the time limit to respond is extended or the request is transferred to another custodian. Failure on the part of a custodian to respond to a request within the 30-day time period is to be treated as a decision to refuse to permit the PHI to be examined or copied.

Furthermore, a custodian must, when requested to do so, provide assistance to an individual in reviewing the individual's PHI. If the custodian is subject to the Official Languages Act, this duty will include an obligation to translate the information to the individual's choice of official language upon request.

PHIPAA does not impose any specific obligation to provide translations of PHI on private custodians. However, private custodians will still be required to assist an individual in interpreting their PHI on request, which may require custodians to explain the information to an individual in another language if the individual cannot understand it in the original language.

A custodian has several options when responding to a request. A custodian must do one of the following:

- make the PHI available for examination and provide a copy, if requested, to the individual;
- inform the individual in writing if the information does not exist or cannot be found;
- inform the individual in writing that the request is refused in whole or in part, provide the specified reason(s) for the refusal and advise the individual of a right to make a complaint about the refusal;
- within 10 days of receiving the request, transfer the request to another custodian if the information requested is maintained by that other custodian, or where the information was originally collected by the other custodian. When a custodian transfers a request, the individual who made the request must be informed of the transfer in writing as soon as possible; or
- in certain circumstances provided for in the Act, where the 30-day time limit is insufficient, extend the time for responding to a request for up to an additional 30 days.

A custodian must take certain precautions about the release of PHI including:

- not permitting PHI to be examined or copied without being satisfied as to the identity of the individual making the request;
- taking reasonable steps to ensure that any PHI intended for an individual is received only by that individual.

The *Right to Information and Protection of Privacy Act* may apply to personal information that is not PHI maintained by a custodian. The specific provisions of the *Right to Information and Protection of Privacy Act* should be reviewed and considered.

Reasons for refusing a request

There are a limited number of circumstances where a custodian may refuse an individual's request to access his or her PHI. These circumstances include:

- if knowledge of the information could reasonably be expected to endanger the health or safety of the individual or another person;
- if disclosure of the information would reveal PHI about another person who has not consented to the disclosure;
- if disclosure of the information could reasonably be expected to identify a third party, other than another custodian, who supplied the information in confidence under circumstances in which confidentiality was reasonably expected;
- if the information was compiled and used solely for one or more of the following purposes:
  - for review by a committee established to study or evaluate the health-care practices of a health-care facility;
  - for a body with statutory responsibility to discipline health-care providers or to regulate the quality or standards of professional services by health-care providers;
  - for risk management or error management;
  - for activities to improve or maintain the quality of care; or to improve or maintain the quality of any related programs or services of the custodian;
- if 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;
- if the information is protected by privilege;
- if another Act of the Legislature of New Brunswick or the Parliament of Canada or a court order prohibits disclosure of the PHI to the individual;

- if the PHI was collected for an investigation conducted pursuant to an Act of the Legislature of New Brunswick; and
- for any reason set out in the regulations.

Before deciding to refuse an individual's request to access PHI, a custodian may consult with another health-care provider(s) who has been involved in the individual's care or any other health-care provider.

In circumstances where a custodian refuses access to PHI for one of the reasons noted, the custodian must, to the extent possible, sever the PHI that cannot be examined or copied and permit the individual to examine and receive a copy of the remainder of the information.

Costs

PHIPAA provides that a custodian must permit an individual to examine a record free of charge. However, a custodian may require an individual to pay a fair and reasonable fee for search, preparation, copying and delivery services. These fees must not exceed the greater of the amount provided for in the regulations and the actual cost of the services provided.

Correction of Personal Health Information

An individual has a right under PHIPAA to request a correction to any PHI examined by the individual to ensure the accuracy and completeness of the PHI. A request for correction must be in writing.

Within 30 days after receiving a request for correction, a custodian must do one of the following:

- make the requested correction to the record of the PHI in such a manner that it will be read with and form part of the record or be adequately cross-referenced;
- inform the individual in writing if the PHI no longer exists or cannot be found;
- if the custodian does not maintain the PHI, advise the individual making the request for correction of this fact; provide the individual making the request with the name and address of the custodian that does maintain the PHI; transfer the request to that custodian; and advise the individual requesting the correction of the transfer; or
- inform the individual in writing of the custodian's refusal to correct the record of PHI with the reason(s) for the refusal and of the individual's right to add a statement of disagreement to the record and to make a complaint about the refusal to correct.

A custodian must make the correction or add any statement of disagreement to any record of PHI maintained by the custodian. The custodian must also notify any other custodian or person to whom the PHI has been disclosed about any correction or statement of disagreement.

A custodian is not permitted to charge a fee in connection with a request for a correction.

Although PHIPAA provides for a formal structure for ensuring an individual's right to examine, copy and correct a record of his or her PHI, PHIPAA also provides for and encourages informal access to PHI. For example, PHIPAA is not intended to prevent a custodian from granting an individual access to a record of his or her own PHI if the individual makes an oral request for access or makes no request, provided that the access is otherwise authorized by PHIPAA, or to prevent a custodian from communicating with the individual about the collection, use or disclosure of his or her PHI.

C. Consent

Consent – General requirements

In general, PHI can only be collected, used, or disclosed by a custodian with the consent of the individual.

The consent provisions set out in PHIPAA also apply to any collection, use or disclosure of PHI by a custodian that requires the consent of the individual under another New Brunswick act.

Under PHIPAA, an individual is considered capable of giving consent only when the individual, at the time at which the decision is made:

- is capable of understanding all of the information relevant to his or her decision of whether to give consent; and
- is capable of appreciating the reasonably foreseeable consequences of consenting or withholding consent.

For consent to be valid, it must meet the following criteria:

- it must be given by the individual, if the individual is capable of giving consent, or by a substitute decision-maker if the individual is not capable of giving consent;
- it must be knowledgeable, in the sense that it must be reasonable in the circumstances for the custodian to believe that the individual knows:
  - the purpose of the collection, use or disclosure;
  - that he or she has the option of giving or withholding consent; and
  - that the information can only be collected, used, or disclosed without his or her consent in accordance with the provisions of PHIPAA.
- the individual must be given the option of withdrawing or withholding his or her consent;
- the consent must relate to the PHI in question; and
- the consent must not be obtained through deception or coercion.

Under PHIPAA's consent rules, consent must, unless otherwise specified in the Act, be expressly given by the individual to be valid. Where a custodian is collecting or using an individual's PHI, or disclosing it to another person, for providing health care to that individual, the custodian may assume (unless it is not reasonable in the circumstances) that the individual has given his or her implied and knowledgeable consent to the collection and use of PHI or to disclose the information to another custodian or person for providing health care to that individual if the scope and purpose of the collection, use and disclosure is evident. Whether express or implied, an individual's consent will continue to be valid until the individual expressly withdraws consent; or, until it otherwise becomes unreasonable to assume that the individual is giving consent under the circumstances.

Implied consent to collection, use and disclosure

Compliance with PHIPAA does not mean that a health-care professional cannot collect, disclose or use PHI for a health-care-related purpose. As previously noted, implied consent to collection, use or disclosure of PHI allows custodians some freedom to appropriately share PHI with other custodians or persons who are involved in providing health care to the individual. This freedom to share PHI will continue to exist only for as long as the custodian continues to have 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 PHI 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-care 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 individuals' continuing implied knowledgeable consent. For example, the Act permits the sharing of an individual's PHI 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 understands his or her rights with respect to providing or withdrawing consent.

The scope of implied consent is strictly limited to only those custodians or other persons involved in providing health care to the individual. PHIPAA imposes strict express consent requirements on any collection, use or disclosure which falls outside of this scope. 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 PHI 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.

Implied knowledgeable consent will only continue to exist for as long as it is reasonable for the custodian to assume that the individual is continuing to consent. An individual can withhold or withdraw his or her continued consent at any time by giving express instructions to the custodian, and if such instructions are given, the custodian will not be able to rely on implied consent to share information with other custodians or health care practitioners.

Substitute decision-makers

PHIPAA allows for persons other than the individual to give or withhold consent in limited circumstances when the individual is incapable of giving consent directly. Custodians are entitled to presume that an individual is capable unless there is some reason to believe otherwise. In general, a custodian should always attempt to obtain consent directly from the individual before resorting to a substitute decision-maker.

Individuals may specifically appoint substitute decision-makers to give or withhold consent for them in the event they become incapable of giving consent. PHIPAA authorizes the following list of persons who may act as a substitute decision-maker, in the event that the individual has not appointed one. They are presented in order from first choice of substitute to last choice – a person lower on the list cannot act as a substitute decision-maker if a person higher on the list is capable of doing so:

- a person who has been authorized in writing by the individual to provide consent;
- a committee of the person appointed under the *Infirm Persons Act* for the individual;
- an attorney for personal care appointed for the individual under the *Infirm Persons Act;*
- an attorney appointed under a power of attorney with respect to property, if the decision relates to the attorney's duties under the power of attorney;
- family members (in all cases, the family member must be an adult to act as a substitute decision-maker):
  - spouse or common-law partner;
  - child;
  - parent or guardian;
  - sibling;
  - grandchild;
  - uncle or aunt;
  - nephew or niece;
  - any other surviving next of kin of the individual;

- the individual's health-care provider; and
- the Public Trustee.

Where the individual in question is deceased, the individual's personal representative may also act as a substitute decision-maker where the decision relates to the administration of the individual's estate.

D. Collection, use and disclosure of personal health information

Introduction

This section of the document is intended to provide a general overview of the rules governing collection, use and disclosure of PHI which are set out in Part 4 of the Act.

PHIPAA does not diminish any other legal duty that may require a custodian to collect, use or disclose PHI. Where a custodian is required by some other statute or by an order of the court to collect, use or disclose PHI without the consent of the individual, the custodian must still comply with that requirement.

The rules in PHIPAA only apply to PHI which is capable of identifying the individual to whom it relates. If PHI information has had all identifying information removed, the de-identified information may be collected, used and disclosed for any purpose, with or without the consent of the individual to whom it relates.

As a general principle, a custodian should only collect, use, or disclose PHI to the minimum extent necessary to fulfil the purpose for the collection, use or disclosure.

Medicare numbers

PHIPAA has special rules relating to Medicare numbers. There are only three purposes for which any person may require the collection, use or production of an individual's Medicare number:

- for provision of health care;
- to verify eligibility for a health-care program or service; and
- for payment and management of the health-care system.

An individual may refuse to provide his or her Medicare number that is not for one of these purposes. This restriction on the collection, use or disclosure of Medicare numbers is one of the few instances in which PHIPAA places restrictions on individuals who may not otherwise be custodians.

Collection of Personal Health Information

As a general principle, a custodian may only collect PHI if the custodian has the individual's consent and the collection is necessary for a lawful purpose; or if the collection is otherwise expressly permitted or required by PHIPAA.

Generally, custodians must collect PHI directly from the individual to whom the information relates. There are a number of situations set out in PHIPAA in which PHI may be collected indirectly from other sources including where:

- another method of collection has been authorized, either by the individual, or by another law or court order;
- direct collection from the individual could endanger the health or safety of the individual or another person;
- the collection is in the interest of the individual and time or circumstances do not permit for collection of the information directly from the individual;
- direct collection could reasonably be expected to result in inaccurate information;

- the information is collected for the purpose of a research project that has been approved by a research review body;
- a substitute decision-maker is acting in place of the individual;
- the information is collected for determining the individual's eligibility for a health-care program or service from the custodian;
- the information is collected for compiling statistical information about the health-care system;
- the information is collected for preparing a family or genetic history for the individual in the course of providing health-care services to that individual; and
- for creating the electronic health record.

Custodians should always try to obtain the individual's consent before collecting PHI. PHIPAA only allows custodians to collect PHI without the consent of the individual in circumstances where an individual is incapable of providing consent, including the following limited number of situations:

- there is no substitute decision-maker for the individual who can provide the consent in a timely fashion;
- the individual is an involuntary patient in a psychiatric facility; or
- the collection is necessary for provision of health care to the individual.

There are a small number of circumstances in which PHIPAA does not allow individuals to refuse or withdraw their consent to collection of information including when the collection is allowed or required by law or when the collection is for the purposes of a program to monitor the prescribing, dispensing or use of certain classes of drugs; is for the creation or maintenance of an electronic health record; or where the collection, use or disclosure is for another purpose provided for in the Act.

Use of personal health information

PHIPAA provides that PHI may be used by custodians in the following circumstances:

- for the purpose for which it was collected or created and for all functions reasonably necessary for that purpose. The individual may limit the custodian's right to use the PHI by giving expressed instructions to the custodian. It should, however, be noted that instructions given by the individual will not limit a custodian's right to use information in the circumstances where the Act permits or requires the custodian to use PHI without consent;
- any use consented to by the individual;
- for obtaining payment, processing, monitoring, verifying or reimbursing claims for payment, or preventing any unauthorized receipt of related services or benefits (which includes debt collection for health care or related goods or services);
- for a research project, as long as the project is approved by a research review body. Research review bodies must meet a number of requirements set out by PHIPAA to be capable of approving research projects;
- for any legal proceeding where the custodian or its agent is, or is expected to be a party or witness, if the PHI relates to the subject matter of the proceeding;
- where the custodian is a regional health authority, the board of directors, management personnel, and administrative or advisory committees of the regional health authority may use PHI for planning and resource allocation; health-system management, public-health surveillance; and health-policy development;
- for a purpose for which another person is permitted or required to disclose this information to the custodian;
- for educating agents to provide health care; and
- for de-identifying PHI.

Disclosure of personal health information

PHI may generally be disclosed to the individual to whom it relates; or, to another party if the custodian has obtained the consent of the individual for the disclosure. PHIPAA sets out a number of other circumstances in which PHI may be disclosed without the consent of the individual including:

- unless the individual has previously instructed otherwise, to the individual's health-care providers in situations where the individual is incapable of giving consent in a timely manner and the disclosure is for providing health care. When an emergent situation exists, health-care professionals can use and disclose an individual's PHI for treating that individual;
- health-care facilities may disclose PHI to their patients' immediate family or to people with whom the individual has a close relationship so long as the disclosure is made in accordance with professional practices. The individual must be given the chance to object to the disclosure at the first reasonable opportunity;
- PHI may be disclosed for identifying deceased individuals or informing family and friends of the deceased;
- to the Minister of Health and to public health authorities needing information for administrative purposes relating to the management of the health-care system, such as recovering health-care costs or monitoring claims for health-care payments;
- in relation to audits or accreditation reviews, where the audit or review relates to services provided by the custodian or for conducting an audit of the custodian's health-care practice; or, for providing legal or risk management services to the custodian;
- in connection with health-care programs for services. For instance: to determine eligibility for a health-care program or to obtain payment for provision of health care. This exception generally only applies to health-care programs or services established by legislation or funded at least partially by the provincial or federal government;
- to other custodians where necessary for review and planning of health care;
- where required for a professional disciplinary or investigative proceeding; or, where otherwise compelled to produce information by the court;
- for a proceeding in which the custodian or its agent is a party or a witness if the information relates to a matter in issue in the proceeding (and, similarly for a contemplated proceeding);
- for educating agents to provide health care; or
- for de-identifying PHI.

Where a custodian discloses information without consent, the custodian must keep a record of the name of the person who received the information, the date and purpose of the disclosure, and a description of the information disclosed. If information is disclosed by permitting access to information stored in an information system, the custodian must ensure that the database automatically keeps an electronic log of the information accessed and individuals accessing the information.

E. Information practices, policy and security

A custodian's information practices include the policies and procedures of the custodian governing its actions in relation to when, how and the purposes for which it routinely collects, uses, modifies, discloses, retains or disposes of PHI and the administrative, technical and physical safeguards and practices that the custodian maintains with respect to that information.

A custodian must establish and implement information practices to facilitate the implementation of, and to ensure compliance with PHIPAA. The custodian must designate a person to assist in ensuring compliance, to respond to inquiries about the custodian's information practices, and to receive complaints from the public. The custodian must promote openness, transparency of policies and procedures to the public.

A list of some of the key requirements for custodians with respect to information practices is provided below. PHIPAA should be consulted for further details regarding a custodian's obligations and duties. This list is not intended to be exhaustive.

Privacy breach reporting

A custodian must provide notification to the Access to Information and Privacy Commissioner and to any individual to whom the PHI relates at the first reasonable opportunity if PHI is stolen, lost, disposed of contrary to PHIPAA or the PHI is disclosed to or accessed by an unauthorized person. PHIPAA provides for an exception to this obligation where the custodian reasonably believes that the breach will not have an adverse impact on the provision of health care or other benefits to the individual to whom the information relates; will not have an adverse impact on his or her mental, physical, economic or social well-being; and will not lead to his or her identification.

Security safeguards

Custodians are required by PHIPAA to:

- protect PHI by implementing reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information. Physical safeguards might include locked filing cabinets and restricted access to offices. Technical safeguards might include encryption and passwords. Administrative safeguards might include developing and implementing privacy and security policies and training programs;
- implement controls that limit the persons who may use the PHI maintained by the custodian to persons specifically authorized by the custodian. Security clearances and limiting access on a "need to know" basis are examples of controls to limit access to and use of PHI;
- implement controls for identification and authentication to ensure that only authorized individuals are allowed to access and use PHI and only for the authorized purposes.;
- implement procedures to prevent the interception of PHI by unauthorized persons where PHI is disclosed or transmitted electronically. For example, using passwords and encryption;
- ensure that each request for disclosure of PHI contains sufficient detail to uniquely identify the individual to whom the information relates;
- ensure that agents adhere to the safeguards; and
- implement any additional safeguards for the security and protection of the information as required by the regulations.

Agents

In addition to the direct obligations PHIPAA places on custodians, PHIPAA imposes specific obligations on custodians with respect to their agents and employees. For example, where a custodian retains the services of an agent for the collection, use, disclosure or retention of PHI, PHIPPA requires the custodian to enter into a written agreement with the agent requiring the agent to comply with the custodian's legal obligations about the handling of PHI.

In addition, PHIPAA imposes a duty on custodians to ensure that agents adhere to the specific safeguards required by the Act.

Information managers

PHI may be provided to an information manager for processing, storing or destroying PHI or providing the custodian with information management or information technology services. The custodian and the information manager must enter into a written agreement that provides for the protection of the PHI against risks such as unauthorized access to or use or disclosure, secure destruction or alteration of the information.

PHIPAA requires the information manager to comply with the duties imposed on the information manager under the written agreement and with the same requirements concerning the protection, retention and secure destruction of PHI that the custodian is required to comply with under PHIPAA. Information managers are also named as custodians under PHIPAA and thus are legally bound by the Act.

Accuracy of information

Before using or disclosing PHI, a custodian must take reasonable steps to ensure that the information is accurate, up-to-date and complete; and to ensure that the disclosure is made to the person intended and authorized to receive the information.

Ceasing operation as a custodian

- A custodian does not cease to be a custodian of PHI until complete custody and control of the record of the PHI passes to another person who is legally authorized to hold the record.
- Where a custodian ceases to be a custodian, there are obligations on the custodian or the custodian's successor to provide notice, including details of where any individual to whom the PHI relates may make a written request for access and the period of time during which the PHI will be maintained.
- The personal representative of a deceased custodian will be required to assume the custodian's obligations upon the custodian's death.

Requirements for retention, storage and secure destruction of information

- Custodians must establish and comply with a written policy for the retention, archival storage, access, and secure destruction of PHI that meets the requirements prescribed by the regulations and New Brunswick law, which would include the regulatory statutes of various health-care professions.
- The policy must protect the privacy of the individual to whom the information relates and requires that a custodian who destroys PHI keep a record of the individual whose PHI 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.

Additional information practices required by public bodies

In addition to the above requirements, if the custodian is a public body (or another custodian specifically named in the regulations), there are obligations under the Act which will generally apply to that custodian, including:

- the requirement to complete a Privacy Impact Assessment (PIA) when there is a new collection, use or disclosure of PHI or when there are any proposed changes to the collection, use or disclosure of PHI or the creation or modification of an information system containing PHI. A PIA is a tool that is used to proactively identify and assess risks associated with the new or modified collection, use or disclosure. A PIA must describe in the form and manner prescribed by the regulations, how the proposed new or changed collection, use or disclosure of PHI may affect the privacy of individuals to whom the information relates. The Commissioner may review PIAs completed by public bodies at his or her discretion; and
- the requirement to store PHI in its custody or control only in Canada, except if the individual has consented to such storage in the other jurisdiction, if the information is stored in the other jurisdiction for disclosure allowed under the Act, or if the information was disclosed for purposes related to making payment to or by the province or a public body.

F. Access to Information and Privacy Commissioner

The Commissioner, appointed under the *Right to Information and Protection of Privacy Act,* is responsible for the administration of PHIPAA. In addition to the Commissioner's duties and powers related to investigating complaints (refer to Section G below), the Commissioner has the power to:

- monitor how PHIPAA is administered;
- conduct investigations to monitor compliance with PHIPAA;
- review PIAs that have been conducted by a custodian that is a public body;
- inform the public about PHIPAA;
- promote best practices and provide advice to custodians;
- make recommendations with regard to PHIPAA; and
- review any matter referred to the Commissioner by the Executive Council.

G. Complaints and review

PHIPAA includes a process by which individuals may complain, either to the Commissioner or in some cases to the court, when they believe that a custodian has improperly handled their PHI.

An individual may make a complaint about a request for access to or correction of PHI to the Commissioner; or, they may refer the complaint directly to the New Brunswick Court of Queen's Bench to request judicial review of the custodian's decision. If an individual decides to refer his or her complaint to the court, the individual cannot also file a complaint with the Commissioner. A matter referred to the court must be filed within 30 days after the date of the custodian's decision.

A complaint may be made to the Commissioner where an individual believes that the custodian has wrongfully collected, used or disclosed his or her PHI, or otherwise failed to keep the information secure. Complaints to the Commissioner must be made in writing within 60 days of the occurrence of the subject matter of the complaint. When a complaint is filed, the Commissioner will notify the custodian and provide him or her with a copy of the complaint.

When the Commissioner receives a complaint, PHIPAA gives the Commissioner broad powers to decide at his or her discretion whether the complaint warrants further investigation; and to take whatever action is necessary to investigate fully and resolve the complaint. The Commissioner may, for example:

- require any custodian to disclose any document or record in his or her possession that is not protected by solicitor-client privilege;
- enter and inspect the custodian's offices; and
- speak with any employees of the custodian.

The Commissioner will usually try to resolve any complaint informally. If the complaint cannot be resolved informally after 45 days, the Commissioner will be required to prepare a report on the complaint with a recommendation on how the problem should be addressed.

The custodian may decide either to accept or reject the Commissioner's recommendation and must inform the individual in writing of its decision within 15 days of receiving the report. If the custodian accepts the recommendation, the custodian must also comply with the recommendation within this 15-day period.

If the custodian rejects the recommendation, the individual may appeal to the court. When the custodian informs the individual of his or her decision to reject the recommendation, the custodian must also inform the individual of this right of appeal.

H. Offences and penalties

PHIPAA creates a number of offences for which a custodian or other person may be prosecuted in court.

PHIPAA prohibits any person, whether or not they are a custodian, from doing any of the following:

- intentionally collecting, using or disclosing PHI in a way that breaches PHIPAA;

- intentionally attempting to gain or gaining access to PHI in a way that breaches PHIPAA;
- knowingly making a false or misleading statement to the Commissioner; or, knowingly attempting to mislead the Commissioner;
- obstructing the Commissioner in the course of performing duties or exercising powers under PHIPAA;
- destroying or erasing a record that is subject to PHIPAA to evade a request to examine or copy the record;
- altering, falsifying, concealing or destroying any record or part of any record, with an intent to evade a request to examine or copy the record; and
- intentionally failing to comply with an investigation of the Commissioner.

In addition to the above, custodians and information managers are considered to have committed an offence if they are found to be:

- collecting, using, selling or disclosing PHI contrary to PHIPAA, unless the custodian took all reasonable steps to prevent the contravention;
- failing to protect PHI in a secure manner as required by PHIPAA, unless the custodian took all reasonable steps to protect the PHI;
- disclosing PHI contrary to PHIPAA with the intent of obtaining a monetary or other material benefit for themselves or some other person; and
- retaliating against their employees for complying with a request or requirement to produce a record or provide information or evidence to the Commissioner or the Commissioner's agent under PHIPAA.

Employees of custodians and information managers who disclose PHI in wilful contravention of PHIPAA will be considered to have committed an offence under the Act unless they have done so with the authorization of the custodian or information manager, in which case the custodian or information manager will be considered to have committed the offence.

PHIPAA defines each of these offences as a Category F offence under the *Provincial Offences Procedures Act*. A judge may impose the following penalties on anyone who is convicted of a Category F offence:

- a minimum fine of $240, which can be increased up to a maximum of $5,120;
- a fine of $7,620 if the offender has previously received the maximum fine for the same offence;
- a sentence of up to 90 days' imprisonment, if the offender has previously been convicted for the same offence and no penalty other than imprisonment will deter the offender from reoffending; and
- if the offender is a corporation, an additional fine of $9,000 may be imposed instead of imprisonment.

Conclusion

PHIPAA will impose a new legislative framework on individuals and organizations defined as custodians under the Act. All custodians, whether they were previously bound by federal or provincial privacy legislation, should carefully review their information practices to ensure that they will be in compliance with the Act and regulations.

Part 3: Comparison of PHIPAA and PIPEDA (for PHIPAA custodians who are already subject to PIPEDA)

Introduction

Custodians such as physicians, dentists and physiotherapists in private practice who are already subject to PIPEDA and who have established information practices that comply with PIPEDA will generally find that most of these practices will meet the requirements of PHIPAA with minimal alterations. There are some key distinctions, however, between the two Acts of which custodians who are already subject to PIPEDA should be aware, and which may require them to modify or enhance their existing practices. These will be highlighted in this part of the paper.

Scope of the Acts

PIPEDA, as federal legislation, applies generally to the collection, use and disclosure of personal information in connection with commercial activities. It applies throughout Canada and across borders subject to some exceptions. PIPEDA applies to all personal information, including PHI, whereas PHIPAA applies only to PHI.

PHIPAA applies to a broader class of health-care activities and organizations than PIPEDA. Whereas PIPEDA applies only to persons or organizations engaged in commercial activities, PHIPAA broadly defines the term custodian and does not distinguish between commercial and non-commercial health-care activities. PHIPAA will apply to all PHI collected, used and maintained by custodians regardless of whether the custodian's activities are commercial. Physicians' activities in private practice, for example, have been subject to PIPEDA since 2004 and will now be subject to PHIPAA. However, the "core activities" of publicly funded hospitals are not subject to PIPEDA but will now be subject to PHIPAA.

Because PHIPAA applies only to PHI and not personal information in general, custodians who are already subject to PIPEDA will not need to change their practices with respect to personal information they may collect, use or disclose for purposes unrelated to an individual's health or provision of health care to comply with PHIPAA.

Types of persons and organizations that will be subject to both PIPEDA and PHIPAA

PIPEDA and PHIPAA will generally apply to custodians (as defined by PHIPAA) who collect, use, disclose or maintain PHI in the course of commercial activities. Some common examples of custodians to whom both Acts may apply include:

- health-care practitioners engaged in private practice such as doctors, nurses, dentists, chiropractors, physiotherapists and opticians;
- pharmacists;
- private companies conducting research for commercial purposes to the extent that research is conducted using PHI;
- nursing homes and operators;
- private laboratories and specimen collection centres; and
- information managers (for example, document storage companies) that collect, use and disclose PHI in the course of providing their services to custodians on a commercial basis.

Appendix A provides further examples of custodians who may be subject to both Acts. Organizations and individuals should consult the Acts and regulations for further guidance and may wish to seek independent legal advice in determining the application of the specific legislation to their particular activities and organizations.

Determining the application of PIPEDA and PHIPAA

When PHIPAA is proclaimed, it will not replace PIPEDA. This means that organizations or individuals considered to be custodians under the PHIPAA and who are subject to PIPEDA will now be subject to both Acts as they relate to their collection, use, and disclosure of PHI.

As federal legislation, PIPEDA is paramount over PHIPAA. This means that where PIPEDA and PHIPAA are in conflict on a particular issue, PHIPAA will not be effective law, and custodians who are subject to both PIPEDA and PHIPAA must comply with PIPEDA. PHIPAA is only effective to the extent that it can be applied without conflicting with PIPEDA.

In determining the specific application of one or both of the Acts with respect to PHI, the following principles may also be applied:

- PIPEDA will continue to apply where PHIPAA is silent or does not address the specific question in issue; and
- where either Act sets out more stringent or more comprehensive legislative requirements on a specific question in issue, then the custodian will have to comply with that particular Act as it relates to its collection, use and disclosure of the PHI in its custody or control (note that in circumstances where PHIPAA is the more stringent or comprehensive of the two Acts, PHIPAA will apply as it relates to its collection, use and disclosure of the PHI in the custodian's custody or control and PIPEDA will continue to apply for the remainder of the personal information that the custodian collects, uses and discloses).

Personal health information definition within PHIPAA and PIPEDA

PHIPAA and PIPEDA define PHI differently. The PHIPAA definition is generally much broader and includes certain types of information that are not expressly included in the PIPEDA definition, such as information that could identify the individual's health-care provider or substitute decision maker. The definitions used in PHIPAA are discussed in greater detail in Part 2 of this paper. Custodians should be aware of the broader definition within PHIPAA when assessing which activities and information will be subject to both Acts.

Individual access to personal health information

Both PIPEDA and PHIPAA grant an individual the right on request to examine or receive a copy of his or her PHI maintained by the custodian. Both require the custodian to respond to requests within 30 days and to provide written reasons to the individual when a request is refused.

PIPEDA requires that requests be made in writing. However, PHIPAA allows some flexibility for individuals and custodians by accommodating both formal written and informal oral requests and allows discretion on the part of the custodian regarding whether an individual must make a request in writing. A written request may be more appropriate, for example, in situations where requests are complex and/or that involve a large volume of PHI and it is preferable for the organization to retain a record of the request. Custodians already subject to PIPEDA will have to consider whether their existing practices can accommodate situations where oral requests may be more appropriate or necessary.

PHIPAA allows a wider range of reasons for which a custodian may refuse a request, such as where the information was collected purely for the purposes of a review by a committee established to study or evaluate the health-care practices of a health-care facility.

However, PIPEDA does not permit an organization to refuse a request for any reason that is not expressly set out in PIPEDA. On the one hand, custodians subject to both Acts must therefore still comply with the narrower list of reasons set out in PIPEDA, and they cannot refuse a request for information for a reason that is allowed by PHIPAA but not PIPEDA. On the other hand, PHIPAA allows custodians to refuse requests for access if the reason for refusal is allowed by another Act. PHIPAA will therefore not limit custodians' ability to refuse requests under PIPEDA.

PIPEDA does not specify or set limits on the fees that a custodian may charge to an individual for access to their personal information, as long as the custodian informs the individual of the approximate fees in advance of providing the requested records and gives the individual an opportunity to withdraw the request. PHIPAA, by contrast, provides that a custodian must permit an individual to examine a record free of charge but is entitled to charge fair and reasonable fees for search, preparation, copying and delivery services if the custodian so chooses. These fees must not exceed the greater of the amount provided for in the regulations and the actual cost of the services provided. Custodians subject to both Acts should consult PHIPAA's regulations once they are available to determine the impact on their current practices with respect to charging fees.

Correction of an individual's personal health information

Under both PHIPAA and PIPEDA, an individual has the right to request that the custodian correct his or her PHI to ensure its accuracy and completeness.

Both PHIPAA and PIPEDA require custodians to keep a record of the reasons for denying the individual's request for correction of a record and to appropriately inform third parties of the nature of the disagreement. However, PHIPAA provides an individual with the right to file a statement of disagreement and to have it placed on the individual's record(s). Custodians subject to both Acts should be aware of this new requirement and adapt their practices to ensure compliance with both Acts.

Consent

Under both PIPEDA and PHIPAA, PHI can generally only be collected, used or disclosed by a custodian with the consent of the individual. Both PIPEDA and PHIPAA provide guidance as to what will constitute a valid consent. For example, both Acts require that consent be knowledgeable and require that the individual must be reasonably able to understand how the information will be used and disclosed. This can be achieved by developing and making readily available a notice that describes the purpose for the collection, use and disclosure of the PHI. Custodians who already have a privacy notice in place should review their existing notice in light of any new requirements of PHIPAA and make the appropriate adjustments.

With respect to consent, PHIPAA provides more specificity and detailed guidance regarding the types of consent required for collection use and disclosure of PHI in various situations, whereas PIPEDA outlines general principles to be considered in determining what type of consent is appropriate in the circumstances. For example, PIPEDA outlines factors that should be considered, such as the sensitivity of the information, the specific circumstances and the type of information collected, whereas PHIPAA provides specific guidance on when express or implied consent will be required as well as situations in which PHI may be collected, used or disclosed without consent. Unlike PIPEDA, for example, PHIPAA clarifies that that unless otherwise provided in the Act, express consent of the individual must be obtained before collecting, using or disclosing PHI, and it provides for the sharing of PHI among health-care professionals for health-care purposes with implied consent. Therefore, in determining the type of consent appropriate for the collection, use and disclosure of PHI in various circumstances and for various purposes, custodians who are also subject to PIPEDA will generally take direction from PHIPAA's more prescriptive consent provisions. Further details on the types of consent required by PHIPAA are in Part 2 of this paper.

Custodians who are already subject to PIPEDA should be aware of the new rules regarding substitute decision-makers. Although PIPEDA provides that consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney), PHIPAA provides a detailed list of persons who may act as a substitute decision-maker for an individual who is incapable of consenting to the collection, use or disclosure of his or her PHI by giving, withholding or withdrawing consent on the individual's behalf.

Both PIPEDA and PHIPAA grant individuals the right to withhold or withdraw consent. This right is subject to certain limitations under both Acts, including legal restrictions. The consent rules under PHIPAA are discussed in greater detail in Part 2 of this paper and should be reviewed by custodians subject to both Acts to determine the impact on their consent management processes.

Collection, use and disclosure of personal health information without consent

The exceptions set out in PHIPAA regarding circumstances in which PHI can be collected, used, and disclosed without the consent of the individual are different from, and more extensive and health-care specific than the general exceptions set out in PIPEDA. The obligations and duties of custodians may vary somewhat between PHIPAA and PIPEDA; therefore, the specific legislation should be consulted to ensure compliance.

PHIPAA is silent with respect to collection of PHI without consent except for situations where the individual is incapable of consent. As a result, custodians who are already subject to PIPEDA can still rely on the more comprehensive list of exceptions to the consent requirement set out in PIPEDA when collecting PHI.

With respect to use and disclosure of personal information without consent, the exceptions set out in PIPEDA take priority over the exceptions in PHIPAA. If a certain collection, use or disclosure of personal information is not expressly permitted by PIPEDA, a custodian who is already subject to PIPEDA will not be allowed to collect, use or disclose the information in that way, even if it would be allowed under PHIPAA. However, PHIPAA may place further limitations on the exceptions set out in PIPEDA. The exceptions to the consent requirement under PHIPAA are reviewed in greater detail in Part 2 of this paper.

PHIPAA has special rules relating to the allowable collection, use and production of Medicare numbers. PIPEDA has no similar rules regarding Medicare numbers. However, a custodian who is already subject to PIPEDA who collects and uses the Medicare number for a health-related purpose should have no need to adjust its practices with respect to Medicare numbers to comply with PHIPAA. The PHIPAA rules regarding Medicare numbers are reviewed in greater detail in Part 2D of this paper.

Information safeguards and practices

The obligations and duties in relation to information management practices and safeguards required by PHIPAA are outlined in Part 2E of this paper. The following is a summary of the key differences between the Acts and some potential implications for custodians.

- Both PHIPAA and PIPEDA require that an individual within an organization be appointed or designated to ensure that the business or organization is compliant with the legislation in connection with the personal information that it collects, uses or discloses. Under PHIPAA, this designated individual's responsibility is to assist the custodian in ensuring compliance; under PIPEDA, the designated individual is directly accountable for ensuring compliance under the Act. Most custodians already subject to PIPEDA should have a Chief Privacy Officer or other privacy officer in place, and will therefore meet the requirements of both Acts.
    - PHIPAA requires several specific procedural safeguards not required by PIPEDA:
        - PHIPAA requires custodians to enter into a written agreement with any agents or information managers who act for or on behalf of the custodian in which the agents or information managers agree to comply with the custodian's duties under PHIPAA. There are other requirements outlined in the Act with respect to information managers. Custodians who are already subject to PIPEDA should review their contractual agreements with any third parties who deal with their PHI in light of the requirements of PHIPAA to ensure compliance with PHIPAA's specific requirements;
        - PHIPAA requires custodians to keep records of any PHI about an individual which the custodian destroys. Custodians should review this requirement in light of their information practices under PIPEDA that requires organizations to implement guidelines and procedures governing the destruction of personal information to determine whether any changes are required;
        - Whereas PIPEDA requires organizations to develop guidelines and implement procedures with respect to the retention of personal information, the requirements of PHIPAA appear to be more onerous and may prompt changes to practices or require policies to be developed or modified. PHIPAA requires custodians to establish and comply with a written policy for the retention, archival storage, access and secure destruction of PHI;

- There are privacy breach reporting requirements under PHIPAA that do not exist under PIPEDA. Custodians will be required to report to both the individual and to the Access to Information and Privacy Commissioner in certain situations when PHI is lost, stolen, or otherwise improperly disposed of, disclosed or accessed. Refer to Part 2E of this paper for further details about when a privacy breach must be reported. Custodians should implement procedures to assess the potential impact of a breach of PHI and to comply with the requirements under the Act for notifying individuals and the Commissioner. Agents and information managers of the custodian should be required to immediately notify the custodian in the event of a breach;
- With respect to security safeguards, both PHIPPA and PIPEDA provide that safeguards should be in place and should be appropriate to the sensitivity of the information to be protected. PHIPAA should be reviewed carefully to determine the specific standards and controls that should be in place to ensure the confidentiality, security, accuracy and integrity of the information. A custodian will then be able to determine if any improvements to existing practices will be required in their particular situation;
- PHIPAA contains rules to prevent the use of PHI for data matching in certain situations. Data matching means creating identifying information by combining de-identified PHI or identifying information from multiple electronic databases or records except in certain specific circumstances authorized by the Act. Custodians should consult the Act for further details if this situation applies to their activities.

Oversight bodies and complaints process

Both PIPEDA and PHIPAA provide for the appointment of Commissioners who are responsible for the administration of their respective legislation. As well, both PIPEDA and PHIPAA establish processes whereby individuals may complain to the respective Commissioner when they believe that their PHI has been improperly collected, used or disclosed.

For custodians who are already subject to PIPEDA, this means that individuals may choose to make their complaint either to the New Brunswick Access to Information and Privacy Commissioner, the Privacy Commissioner of Canada or to both. PHIPAA allows individuals to refer a complaint with respect to a custodian's decision regarding the individual's request for access to or correction of his or her record containing PHI to the New Brunswick Court of Queen's Bench rather than making a complaint to a Commissioner. The complaints process under PHIPAA is reviewed in greater detail in Part 2G of this paper. The PIPEDA and PHIPAA complaints processes will not affect each other, but are separate processes under two Acts that can be pursued independently of each other.

Offences and penalties

Both PIPEDA and PHIPAA establish remedies for contraventions of the legislation. The offences created by PHIPAA are in addition to the offences created by PIPEDA, not a replacement. This means that a custodian who is already subject to PIPEDA who improperly collects, uses, or discloses PHI may be charged with both federal and provincial offences. The offences created by PHIPAA are reviewed in greater detail in Part 2H of this paper.

Regulations

The Legislature of New Brunswick is expected to enact regulations to PHIPAA. These may create further distinctions between PHIPAA and PIPEDA, with which custodians who are already subject to PIPEDA will need to comply. For instance, PHIPAA authorizes the making of regulations pertaining to the establishment of electronic health records (EHRs) and prescribing additional safeguards for PHI maintained in electronic form.

PIPEDA appears to be silent with respect to EHR's, in that there are no regulations yet in force pertaining to protecting personal information that may be contained in EHR's.

APPENDIX A – Application of PIPEDA and PHIPAA

TYPES OF INDIVIDUALS OR ORGANIZATIONS	PIPEDA	PHIPAA
Ambulance New Brunswick Inc.		√
Ambulance Services (private-for profit)	√	√
Canadian Blood Services	√	√
Chiropractors in private practice	√	√
Community health centres		√
Dentists in private practice	√	√
Information managers (for instance, information technology service providers, records storage and disposal companies)	* Possibly depending on whether activities are commercial in nature	√
Insurance companies	√	
PHI collected by employers pertaining to employees	* PIPEDA will apply in certain limited organizations only	
Laboratory or specimen collection centres (private-for profit)	√	√
Private medical clinics	√	√
Opticians or optometrists operating private businesses	√	√
Pharmacies	√	√
Medical supplies business	√	
Nurses working in public hospitals		*the hospital is considered the custodian subject to PHIPAA and the nurse would be considered an agent
Nursing homes and their operators	√	√

TYPES OF INDIVIDUALS OR ORGANIZATIONS	PIPEDA	PHIPAA
Special-care homes and their operators	√	√
Public bodies (including but not limited to government departments and crown corporations)		√
Physicians in private practice	√	√
Physicians employed by a hospital or a non-profit health-care organization		*the hospital is considered the custodian subject to PHIPAA and the physician would be considered an agent
Public hospitals and regional health authorities		√
Facilicorp NB Ltd.		√
WorkSafe NB		√