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

This document is intended to respond to some frequently asked questions about the *Personal Health Information Privacy and Access Act (*PHIPAA). It should not be interpreted as legal advice.

1. Why was a new Act needed?

Health information is one of the most sensitive forms of personal information. It is used for a number of purposes: 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.

Privacy legislation at the provincial and federal levels is generally broad in application. Although such pieces of legislation apply to personal information, including personal health information, they do not address many of the specific needs of health-care professionals and organizations in the health-care system that collect, use or disclose personal health information for health-care purposes.

PHIPAA is intended to address these concerns: It is personal health information legislation specific to New Brunswick.

2. What is the purpose of the 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-care system in New Brunswick. It applies to personal health information in the health-care 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 the rights are respected.

PHIPAA places obligations on organizations and individuals that govern how they are permitted and required to collect, use, maintain, disclose and dispose of personal health information to protect the privacy of individuals' personal health information. It is also intended to ensure that these organizations and individuals are accountable to safeguard the security and integrity of personal health information in their possession or under their control.

3. Who must abide by the Act?

Custodians
PHIPAA applies generally to a group of stakeholders throughout the health-care 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;
- hospitals;
- health care providers (for example, physicians, dentists, nurses, pharmacists);
- public bodies (including but not limited to government departments and Crown corporations);
- WorkSafe NB;
- ambulance operators; and
- individuals or organizations known as information managers that manage personal health information on behalf of another custodian.

The law 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 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:

- the 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. Will the Act apply whenever my personal health information is collected, used or maintained?

No. When personal health information is collected, used or maintained by an individual or an organization for purposes other than health care or treatment, the planning and management of the health-care system, or for delivering a government program or service, the Act will not apply. Specifically excluded, unless otherwise stated in the regulations, are 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 may collect personal health information about an individual 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, the Act will not apply. The collection, use, and disclosure of an individual's personal health information may, however, be subject to other federal or provincial privacy legislation, depending on the circumstances.

6. Does the Act introduce restrictions on the collection and use of my Medicare card?

Yes. The Act introduces restrictions on the collection and use of 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 a person'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 Act provides that any person who requests a Medicare number from an individual must advise this individual of his or her authority to do so.

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

The Act identifies several rules that custodians must follow in the collection, use, disclosure, secure destruction and protection of personal health information. 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 about consent, refer to Question 8;
- 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 the proper use and disclosure of information in accordance with the Act;
- establish and implement appropriate policies and practices that will protect the integrity, confidentiality, security and accuracy of personal health information;
- where outside service providers are used to process personal health information on the custodian's behalf, follow specific rules to ensure that this information is appropriately protected while it is processed at the other organization; and
- if identifiable personal health information about a person is stolen, lost or used contrary to PHIPAA, a custodian may be required to notify this person and the Access to Information and Privacy Commissioner.

8. How does the Act protect against improper use and disclosure of my 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 disclosing personal health information.

The Act protects privacy by placing limits on the collection, use, disclosure, and destruction of personal health information. In particular:

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

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 for the provision of health services to the individual. The Act 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, an individual must first have been informed about the purpose of the collection, use and disclosure; and he or she must be aware he or she has a choice to give, withhold or withdraw consent to the collection, use or disclosure of his or her 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, he or she will be considered to have been appropriately informed.

These provisions ensure that health providers who need to know pertinent information about a person to provide proper care and treatment are entitled to continue to use that information for those purposes as long as they have that person's continuing implied knowledgeable consent. For example, the Act permits the sharing of personal health information between a specialist and a family physician when a person is being treated in hospital as long as this person 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 Act 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 exist 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.

Disclosure without consent in limited circumstances only
PHIPAA provides limited circumstances when personal health information can 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. For other purposes not provided for in the Act or otherwise provided for by law, the Act clearly states that the express consent of the individual must be obtained.

9. If a health custodian who collects and maintains my information outsources information technology or information processing functions, how can I be assured that my information is protected?

The Act allows custodians to provide personal health information to an outside service provider (defined as an information manager under the Act) for processing, storing or destroying that information on its behalf or providing the custodian with information management or information technology services.

However, the Act requires custodians to follow specific rules to ensure that personal health information is appropriately protected while it is processed at the other organization. This includes requiring the information manager and the custodian to enter into and comply with the terms of a written agreement outlining the specific safeguards that an information manager must have in place to ensure the protection, security and confidentiality of the personal health information it manages on behalf of the custodian. Information managers must acknowledge that they are required to comply with the Act and, as such, are prohibited from disclosing any personal health information to which they are provided access. They must only use the personal health information for providing the services and not for any other uses.

10. Will this Act change the way my personal health information is protected?

The Act builds on existing practice to improve the protection of personal health information. For example, the Act:

- standardizes information practices in the health-care system;
- gives individuals the right to request access to and corrections of their health information anywhere in the health-care system;
- adds legal limits to accessing and using personal health information. Even within the walls of a single organization or health-care facility, only those who need to know can access and use the information;
- places limits on the collection and use of Medicare numbers;
- designates an independent third party (the Access to Information and Privacy Commissioner) to investigate breaches and complaints about the treatment of personal health information and to oversee compliance with and education about the Act;
- requires that custodians adopt information practices including appropriate policies to ensure the security, confidentiality, accuracy and appropriate retention and destruction of personal health information;
- places stringent requirements on information managers who process or maintain personal health information on behalf of custodians, ensuring that the same level of protection is in place at these organizations or with these individuals as the custodians are required to comply with under the Act;
- ensures that individuals are informed if their personal health information has been lost, stolen or used inappropriately where it is reasonable to believe that their well-being or the provision of health care may be impaired and in cases that could lead to identification of the individual;
- establishes rules for the sharing of personal health information among custodians within an information network; and
- establishes very serious penalties for abuse of personal health information.

11. What are my individual rights under the Act ?

PHIPAA identifies specific rights for individuals with respect to their personal health information. Your rights are important because they ensure that you will be involved in decisions about your personal health information.

You have the right to:

- be informed about the purpose for the collection and the anticipated uses and disclosures of your personal health information;
- withhold or withdraw consent for the collection, use and disclosure of your personal health information except in specific circumstances outlined in the Act;
- designate another person to make decisions about their personal health information;
- request to examine or receive a copy of your personal health information (which may be subject to a fee, as outlined in the Act and regulations);
- request correction of your personal health information once you have examined it;
- refuse to provide your Medicare number to any person or organization that collects the information as identification for a non-health service;
- 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.
- appeal or refer a matter to court; and
- be informed if your 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 you.

12. How can I obtain access, or request a correction to, my personal health information record?

You are entitled to request access to your information that you believe to be in the possession of a custodian. You will need to provide sufficient detail to permit the custodian to identify and locate the record(s) being sought. A custodian may require you to make your request in writing.

A custodian must generally respond to a request no later than 30 days after receiving it, unless the custodians needs an extension, in which case they must notify you. A custodian may require an extension if, for example, a large number of records has been requested or must be searched, or if more time is needed to consult with a third-party or another custodian. In some cases, a custodian may refer a request for access to another custodian if the information is maintained or was first collected by the other custodian.

In responding to a request, a custodian must:

- make information available to the individual for examination or provide a copy if it has been requested;
- 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, reasons for denying access must be provided. Exceptions may include, for example, information that contains references to other individuals or information subject to solicitor-client or litigation privilege.
- if the individual does not agree with the custodian's decision, he or she has a right to file a complaint with the Access to Information and Privacy Commissioner or to refer the matter to court.

Depending on the nature of the request, the individual may be required to pay a fee.

If the individual believes there is an inaccuracy in the personal health information that a custodian holds about him or her, he or she may request that the custodian make a correction. If the request is approved, the custodian must make the correction to the records they maintain about the individual. If the request is denied, the custodian must provide the reasons and explain how the individual may request a review of the decision.

13. What is an information network? How will the Act protect the privacy of personal health information on 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 which 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 will be protected in a number of ways. The following facts are important to know:

- the minister of Health is accountable for designating information networks under the Act according to the terms of the legislation. As information networks are designated under the Act, information including their purpose and the nature of the information to be collected and used will be posted to the Department of Health's website;
- sharing of information within an information network is only permitted among health-care custodians within the circle of care and only for the specific purposes outlined in the Act. Therefore, the same rules apply to disclosure of personal health information regardless of whether the information is shared within or outside of an information network;

- the custodian of the information network must ensure that only those individuals who need to know the information to accomplish the stated health-care purpose are provided access to the network;
- documentation must be in place regarding all aspects of information management for all health information systems designated as information networks;
- although a custodian is not required to obtain consent of the individual for creating and maintaining an information network, an individual may register a consent directive within an information network to prevent disclosure of your personal health information to a user who would otherwise have access; and
- applications for consent directives must be submitted in writing to the administrator of the information network and will be effective once registered in the information network. A consent directive may only be changed or revoked with written notice to the administrator. It is important to note that a consent directive will be applied to the entire content of an individual's record as opposed to specific parts of an individual's record within an information network.

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

The Act provides that a custodian is 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 his or her 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 consent. An individual may expressly instruct a 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 required by law or otherwise authorized under the Act, and so they may be overridden in certain circumstances. For example, the Act provides that a 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 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 unable to provide 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 steps 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.

16. 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:

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