SUBJECT — Corporate Privacy Policy

NOTE: This is a joint policy of the Chief Privacy Officers' Working Group and shall not be modified except by agreement of that group.

INTRODUCTION

Each of Regional Health Authorities, FacilicorpNB and Ambulance NB, as health system partners (herein referred to as the "Partners") is committed to collecting, using, disclosing and disposing of personal information (PI) and personal health information (PHI) entrusted to us in a manner that is accurate, confidential, secure and private.

As public bodies, the Partners subscribe to the **Canadian Standards Association's Model Code for the Protection of Personal Information**. Ten interrelated privacy principles form the basis of the Code. This policy uses these ten privacy principles, together with applicable privacy legislation, as a foundation for all matters related to privacy and confidentiality.

OBJECTIVE

The purpose of this Policy is to:

- clearly articulate the responsibilities of the Partners in relation to PI and PHI;
- define the privacy principles common to all Partners in the health care system in New Brunswick;
- promote and strengthen accountability for good privacy management practices and foster a culture of privacy among personnel; and
- provide increased confidence in the Partners' effectiveness in identifying and mitigating privacy risks and ensuring compliance with privacy policies, legislation, and regulations.

SCOPE

This Policy applies wherever the Partners' employees or non-staff personnel are engaged in activities where such individuals have access to confidential information including PI and PHI.

The responsibility of the Partners in relation to personal information as defined by the *Right to Information and Protection of Privacy Act* (*RTIPPA*) are set out by such privacy and access policies as may be published by the Province of New Brunswick from time to time, and are outside the scope of this Policy.

LEGISLATIVE REQUIREMENTS

The Partners are subject to and must comply with the *Right to Information and Protection of Privacy Act* (*RTIPPA*) and the *Personal Health Information Privacy and Access Act (PHIPAA)* and their regulations.

DEFINITIONS

"confidential information" includes, but is not limited to, the following information types:

- Personal information (PI)
- Personal health information (PHI)
- Sensitive / proprietary information (i.e., administrative information documented in personal notebooks / diaries)
- Human Resources / Payroll
- Legal
- Financial

"**non-staff personnel**" includes, but is not limited to, agents, board members, students, volunteers, physicians, consultants, third-party service providers, external professionals or experts contracted to offer a service and vendors, demonstrating, installing or servicing equipment, software applications or hardware.

"**personal health information**" means identifying information about an individual in oral or recorded form if the information:

(*a*) relates to the individual's physical or mental health, family history or health care history, including genetic information about the individual,
(*b*) is the individual's registration information, including the Medicare number of the individual,
(*c*) relates to the provision of health care to the individual,
(*d*) relates to information about payments or eligibility for health care in respect of the individual, or eligibility for coverage for health care in respect of the individual,
(*e*) relates to the donation by the 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,
(*f*) identifies the individual's substitute decision-maker, or
(*g*) identifies an individual's health care provider.

PHI is distinguished from personal information by the circumstances in which it was collected. PHI is collected by custodians, typically health care providers in the course of providing health related services to individuals, and public bodies that are part of the health care system. Personal information, such as name and address, is considered PHI when it is collected and retained in connection with these activities. If a non-custodian under *PHIPAA* deals with that same information, it is considered "personal information" subject to the *Right to Information and Protection of Privacy Act* (*RTIPPA*). Further, a custodian under *PHIPAA* will be subject to *RTIPPA* insofar as they may collect personal information. For example, personal information might include occupational and financial circumstances, ethnic, religious or political information, or the personal views or opinions of an individual.

"**personal information**" means recorded information about an identifiable individual, including but not limited to,

(*a*) the individual's name,
(*b*) the individual's home address or electronic mail address or home telephone or facsimile number,
(*c*) information about the individual's age, gender, sexual orientation, marital status or family status,
(*d*) information about the individual's ancestry, race, colour, nationality or national or ethnic origin,
(*e*) information about the individual's religion or creed or religious belief, association or activity,
(*f*) personal health information about the individual,
(*g*) the individual's blood type, fingerprints or other hereditary

characteristics,

(*h*) information about the individual's political belief, association or activity,

(*i*) information about the individual's education, employment or occupation or educational, employment or occupational history,

(*j*) information about the individual's source of income or financial circumstances, activities or history,

(*k*) information about the individual's criminal history, including regulatory offences,

(*l*) the individual's own personal views or opinions, except if they are about another person,

(*m*) the views or opinions expressed about the individual by another person, and

(*n*) an identifying number, symbol or other particular assigned to the individual.

POLICY STATEMENT

The Partners are committed to maintaining common policies, to guide the Partners in protecting confidentiality and privacy.

The Partners recognize the **Canadian Standards Association's Model Code for the Protection of Personal Information** as the foundation for privacy protection.

These principles are:

Principle 1: Accountability
A public body is responsible for personal information under its control. The chief executive officer of a public body, and his or her designates, are accountable for the public body's compliance with the following principles.

Principle 2: Identifying Purposes
The purposes for which personal information is collected shall be identified by the public body at or before the time the information is collected.

Principle 3: Consent
The consent of the individual is required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4: Limiting Collection
The collection of personal information shall be limited to that which is necessary for the purposes identified by the public body. Information shall be collected by fair and lawful means.

Principle 5: Limiting Use, Disclosure and Retention
Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required or expressly authorized by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Principle 6: Accuracy
Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7: Safeguards
Personal information shall be protected by safeguards appropriate to the sensitivity of the information.

Principle 8: Openness
A public body shall make readily available to individuals specific information

about its policies and practices relating to the management of personal information.

Principle 9: Individual Access
Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information, except where inappropriate. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10: Challenging Compliance
An individual shall be able to address a challenge concerning compliance with the above principles to the individual or individuals accountable for the public body's compliance.

ACCOUNTABILITIES

Accountability for management of PI and PHI rests with the respective CEO's of the other Partners. The Chief Privacy Officers of each Partner have been delegated to act on behalf of its CEO, as the case may be.

Partners' employees and non-staff personnel are required to comply with the Partners' privacy policies.

REFERENCES AND ASSOCIATED DOCUMENTS

- *Right to Information and Protection of Privacy Act* (*RTIPPA*)
- *Personal Health Information Privacy and Access Act* (*PHIPAA*)

INQUIRIES

For more information on this Policy, please contact the Chief Privacy Officer for **FacilicorpNB,** Kelly Steeves, at (506) 663-2500.