

Policy Number:	PR - 004	Draft Date:	
Section:	General Administration	Original Date:	November 2010
Issued by:	Privacy	Revision Date(s):	October 2011
Approved by:	Board of Directors		Page 1 of 3

Policy and Procedures

Privacy Impact Assessment 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 the Regional Health Authorities (RHAs), 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.

OBJECTIVE

- ensure that privacy protection is a core consideration in the initial framing of program or service objectives and in all subsequent activities;
- determine the process and requirements by which the Partner conducts Privacy Impact Assessments (**PIA**).
- design privacy into Partner projects and initiatives by identifying and managing risks, and develop projects which enable business processes to enhance the privacy of PHI; and
- ensure that the results of PIAs are communicated to senior management, project sponsors and stakeholders to promote fully-informed policy, program, system and procurement decisions.

SCOPE

This policy applies wherever the Partner's employees or non-staff personnel are engaged in activities related to projects and initiatives which may impact the privacy of PHI in a Partner's care.

LEGISLATIVE REQUIREMENTS

Section 56 of the *Personal Health Information Privacy and Access Act* prescribes circumstances under which public bodies will conduct privacy impact assessments.

DEFINITIONS

Business Owner – person designated by a Partner as being responsible for a program or data system, including development and implementation.

"New Brunswick Department of Health Privacy Impact Assessment Methodology, Guidelines and Tools" – key reference document to conduct a Privacy Impact Assessment (PIA).

"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,

Policy Number:	PR - 004	Draft Date:	
Section:	General Administration	Original Date:	November 2010
Issued by:	Privacy	Revision Date(s):	October 2011
Approved by:	Board of Directors		Page 2 of 3

Policy and Procedures

- (f) identifies the individual's substitute decision-maker, or
- (g) identifies an individual's health care provider.

POLICY STATEMENT

The Partners are responsible for demonstrating that the collection, use and disclosure of PHI respects the legislative requirements, and privacy principles throughout the initiation, analysis, design, development, implementation and post-implementation review phases of all projects and initiatives.

PROCEDURES

1. Determining When PIAs Are Required

A PIA will be commenced and completed at the earliest possible stage in the design and development of the project or initiative, and in any event prior to its deployment.

A Partner will conduct a privacy impact assessment:

- On a new project or initiative that involves the collection, use or disclosure of PHI;
- On an existing project or initiative whenever it involves a significant change in the way in which it handles PHI. Such changes may relate to the key business models, functionality, access, stakeholders or technology associated with such project or initiative; and
- On all activities that involve data linking or data matching.

A Partner may conduct a privacy impact assessment:

- On an existing program or initiative for which no changes are proposed if no previous assessment exists or if there are outstanding privacy issues; and
- On any initiative or solution which the Chief Privacy Officer identifies as requiring analysis for determination of privacy risk.

The scope and necessity of conducting a PIA will be determined by completing the "**PIA Assessment Form**", which must be submitted to your Chief Privacy Officer for formal recommendation. This form is included in the *New Brunswick Department of Health PIA Methodology, Guidelines and Tools* document, available from your Chief Privacy Officer.

Where appropriate, an alternative process may be followed with the approval of the Chief Privacy Officer.

2. Privacy Impact Assessment

When a PIA is required, the *New Brunswick Department of Health PIA Methodology, Guideline and Tools* document must be followed (except where an alternate process has been developed and approved by the Chief Privacy Officer).

The final PIA Report must be submitted to the Chief Privacy Officer for your organization, for formal review and recommendation. The CPO will communicate his or her recommendations, as required.

ACCOUNTABILITIES

Chief Privacy Officer is responsible for:

- implementing, interpreting and enforcing this Policy;
- facilitating the completion of PIAs;
- maintaining current tools and templates for PIA reports and summaries;

Policy Number:	PR - 004	Draft Date:	
Section:	General Administration	Original Date:	November 2010
Issued by:	Privacy	Revision Date(s):	October 2011
Approved by:	Board of Directors		Page 3 of 3

Policy and Procedures

- reviewing of final PIAs by providing written recommendations ensuring that all completed, final PIAs are retained in one location.

Business Owners are responsible for

- ensuring that the Chief Privacy Officer is informed of new initiatives or projects that may require a PIA;
- ensuring that responsible parties allocate sufficient time and funds in their project plans to conduct the PIA; and
- implementing the PIA recommendations and monitoring of privacy risk mitigation strategies.
- **Partner's Employees and Non-Staff Personnel** are responsible to comply with this Policy. A Partner may apply sanctions to employees or non-staff personnel acting on its behalf found in violation of this Policy, consistent with the Partner's disciplinary policies and procedures.

REFERENCES AND ASSOCIATED DOCUMENTS

- *Personal Health Information Privacy and Access Act, (PHIPPA)*;
- Corporate Privacy Policy