

1 *New Brunswick Regulation 2010-111 under the Right to Information and Protection of Privacy Act is amended by adding after section 4 the following:*

Agreements for common or integrated services, programs or activities

4.1(1) For the purposes of paragraph 46.2(2)(b) of the Act, a written agreement entered into for the provision of a common or integrated service, program or activity shall contain the following information:

- (a) a description of the service, program or activity;
- (b) a description of the purposes or expected outcomes or benefits of the service, program or activity;
- (c) a description of the respective roles and responsibilities of each party to the agreement;
- (d) a description of the types of personal information that are to be collected, used or disclosed by each party in the course of providing the service, program or activity and, for each type of personal information,

(i) the purpose for its collection, use or disclosure and the authority under which it is collected, used or disclosed, and

(ii) a description of the manner in which the personal information is to be transferred between the parties;

(e) a summary of the information practices established by each party in order to ensure compliance with paragraph 46.2(2)(a) of the Act; and

(f) the date on which the service, program or activity will start and, if applicable, the date on which the service, program or activity will end.

4.1(2) When a party to a written agreement withdraws from the agreement,

(a) no personal information under the agreement shall be used or disclosed, except

(i) with the prior consent of the person to whom the personal information relates, or

(ii) when required or authorized by law, and

(b) the party shall comply with the information practices in effect immediately before it withdrew from the agreement for as long as the personal information is in its custody or under its control.

Information practices

4.2(1) This section applies to the security arrangements made by a public body under section 48.1 of the Act or under this Regulation with respect to personal information under its custody or under its control.

4.2(2) The security arrangements made by a public body to protect personal information shall be appropriate taking into consideration the degree of assessed risk of unauthorized access, use, disclosure or disposal of the personal information and the degree of harm that could result from the unauthorized access, use, disclosure or disposal of the personal information.

4.2(3) A public body shall make the following security arrangements with respect to personal information:

- (a) maintain lists of
 - (i) the names of its officers, directors, employees or agents who are authorized to access the personal information,
 - (ii) the categories of personal information to which the authorized officers, directors, employees or agents have access, and
 - (iii) the types of access permitted to the personal information by the officers, directors, employees or agents;
- (b) only allow access to the personal information to persons authorized in accordance with paragraph (a);
- (c) provide for a procedure for the verification of the identity of persons seeking access to personal information;
- (d) record and monitor access to the personal information;
- (e) with respect to personal information in paper form, keep the personal information in a secure location;

- (f) with respect to personal information in electronic form, secure the personal information by the use of encryption while the information is stored or being transferred;
- (g) that when responding to requests for disclosure of personal information under the Act, ensure that the request contains sufficient detail to uniquely identify the individual to whom the information relates;
- (h) require the agents of the public body to adhere to the security arrangements made by the public body under the Act and this Regulation; and
- (i) annually test and evaluate the effectiveness of the security arrangements the public body makes under the Act and this Regulation.

4.2(4) A public body shall establish the following measures with respect to incidents of unauthorized access, use, disclosure or disposal of personal information:

- (a) investigate every incident of unauthorized access, use, disclosure or disposal of personal information;
- (b) maintain a registry of every incident and any corrective measure taken in relation to the incident to diminish the likelihood of a similar occurrence;
- (c) notify the person to whom the information relates of any incident that could create a risk of significant harm to the person; and
- (d) notify the Commissioner of any incident under paragraph (c).

4.2(5) For the purposes of paragraph (4)(c), the public body shall take into account the following factors when determining the risk of significant harm to the person:

- (a) the sensitivity of the personal information, and

(b) the probability that the personal information has been, is being, or will be misused.

4.2(6) For greater certainty, a public body shall retain and dispose of personal information in its custody in accordance with the record schedules established by the Provincial Archivist under the *Archives Act*.

2 *This Regulation comes into force on XXXX, 2018.*

DRAFT
ÉBAUCHE