Canadian Privacy Statutes: Provisions with Implications for Information Management

ALBERTA PIPA	BC PIPA	PIPEDA (Part 1)
1. Definitions		
1(k) "personal information" means information about an identifiable individual;	"personal information" means information about an identifiable individual and includes employee personal information but does not include (a) contact information, or (b) work product information;	"personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.
1(m) "record" means a record of information in any form or in any medium, whether in written, printed, photographic or electronic form or any other form, but does not include a computer program or other mechanism that can produce a record;	"document" includes (a) a thing on or by which information is stored, and (b) a document in electronic or similar form	"record" includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.
2. Reasonableness		
2 Where in this Act anything or any matter (a) is described, characterized or referred to as reasonable or unreasonable, or (b) is required or directed to be carried out or otherwise dealt with reasonably or in a reasonable manner, the standard to be applied under this Act in determining whether the thing or matter is reasonable or unreasonable, or has been carried out or otherwise dealt with reasonably or in a reasonable manner, is what a reasonable person would consider appropriate in the circumstances.	4(1) In meeting its responsibilities under this Act, an organization must consider what a reasonable person would consider appropriate in the circumstances.	5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.
3. Purpose of the Act		
3 The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable.	2 The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.	3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.
4. Organization responsible for personal information under its control		
5(1) An organization is responsible for personal information that is in its custody or under its control.	4(2) An organization is responsible for personal information under its control, including personal information that is not in the custody of the organization.	5. (1) Subject to section 6 to 9, every organization shall comply with the obligations set out in Schedule 1. Schedule 1 - 4.1 (Accountability) An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

ALBERTA PIPA	BC PIPA	PIPEDA (Part 1)
5(2) For the purposes of this Act, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with the Act.	4(2) as above.	Schedule 1 - 4.1.3 An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
5(5) In meeting its responsibilities under this Act, an organization must act in a reasonable manner.	4(1) In meeting its responsibilities under this Act, an organization must consider what a reasonable person would consider appropriate in the circumstances.	5. (3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances
5. Policies		
6 An organization must (a) develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act, and	5 An organization must (a) develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under this Act,	Schedule 1 - 4.1.4 Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; ... (c) training staff and communicating to staff information about the organization's policies and practices; and (d) developing information to explain the organization's policies and procedures.
6. Access to personal information		
24(1) Subject to subsections (2) to (4), on the request of an individual for access to personal information about the individual and taking into consideration what is reasonable, an organization must provide the individual with access to the following: (a) the individual's personal information where that information is contained in a record that is in the custody or under the control of the organization; (b) the purposes for which the personal information referred to in clause (a) has been and is being used by the organization; (c) the names of the persons to whom and circumstances in which the personal information referred to in clause (a) has been and is being disclosed.	23 (1) Subject to subsections (2) to (5), on request of an individual, an organization must provide the individual with the following: (a) the individual's personal information under the control of the organization; (b) information about the ways in which the personal information referred to in paragraph (a) has been and is being used by the organization; (c) the names of the individuals and organizations to whom the personal information referred to in paragraph (a) has been disclosed by the organization.	Schedule 1 - 4.9 (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. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. Schedule 1 - 4.9.1 Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed. Schedule 1 – 4.9.3 In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the

ALBERTA PIPA	BC PIPA	PIPEDA (Part 1)
	23(2) An organization that **(a)** is a credit reporting agency, and **(b)** receives a request under subsection (1) must also provide the individual with the names of the sources from which it received the personal information unless it is reasonable to assume the individual can ascertain those sources.	organization shall provide a list of organizations to which it may have disclosed information about the individual. 2. (2) In this Part, a reference to clause 4.3 or 4.9 of Schedule 1 does not include a reference to the note that accompanies that clause.
7. Correction of personal information		
25(1) An individual may request an organization to correct an error or omission in the personal information about the individual that is under the control of the organization.	24 (1) An individual may request an organization to correct an error or omission in the personal information that is (a) about the individual, and (b) under the control of the organization.	Schedule 1 - 4.9 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. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
25(2) If there is an error or omission in personal information in respect of which a request for a correction is received by an organization under subsection (1), the organization must, subject to subsection (3), (a) correct the information as soon as reasonably possible, and (b) where the organization has disclosed the incorrect information to other organizations, send a notification containing the corrected information to each organization to which the incorrect information has been disclosed, if it is reasonable to do so.	24(2) If an organization is satisfied on reasonable grounds that a request made under subsection (1) should be implemented, the organization must (a) correct the personal information as soon as reasonably possible, and (b) send the corrected personal information to each organization to which the personal information was disclosed by the organization during the year before the date the correction was made.	Schedule 1 - 4.9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.
25(3) If an organization makes a determination not to make the correction under subsection (2)(a), the organization must annotate the personal information under its control with the correction that was requested but not made.	24(3) If no correction is made under subsection (2), the organization must annotate the personal information under its control with the correction that was requested but not made.	Schedule 1 – 4.9.6 When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.
25(4) On receiving a notification under subsection (2)(b) containing corrected personal information, an organization must correct the personal information in its custody or under its control.	24(4) When an organization is notified under subsection (2) of a correction of personal information, the organization must correct the personal information under its control.	
8. Accuracy		
33 An organization must make a reasonable effort to ensure that any personal information collected, used or disclosed by or on behalf of an organization is accurate and complete.	33 An organization must make a reasonable effort to ensure that personal information collected by or on behalf of the organization is accurate and complete, if the personal information (a) is likely to be used by the organization to make a decision that affects the individual to whom the personal information relates, or (b) is likely to be disclosed by the organization to another organization.	Schedule 1 - 4.6 (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. Schedule 1 - 4.6.1 The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

ALBERTA PIPA	BC PIPA	PIPEDA (Part 1)
		Schedule 1 - 4.6.2 An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected. Schedule 1 - 4.6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.
9. Security		
34 An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.	34 An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.	Schedule 1 - 4.7 (Safeguards) Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. Schedule 1 - 4.7.1 The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held. Schedule 1 – 4.7.2 The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4. Schedule 1 - 4.7.3 The methods of protection should include (a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis, and (c) technological measures, for example, the use of passwords and encryption. Schedule 1 - 4.7.4 Organizations shall make their employees aware of the importance of maintaining confidentiality of personal information. Schedule 1 - 4.7.5 Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).
10. Retention		
	35(1) Despite subsection (2), if an organization uses an individual's personal information to make a decision that directly affects the individual, the organization must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain	Schedule 1 - 4.5.2 (Limiting Use, Disclosure, and Retention) Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal

ALBERTA PIPA	BC PIPA	PIPEDA (Part 1)
	access to it.	information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.
35 Notwithstanding that a consent has been withdrawn or varied under section 9, an organization may for legal or business purposes retain personal information as long as is reasonable.	35(2) An organization must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that (a) the purpose for which that personal information was collected is no longer being served by retention of the personal information, and (b) retention is no longer necessary for legal or business purposes.	Schedule 1 – 4.5 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 by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes. Schedule 1 - 4.5.3 Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. Schedule 4.5.4: This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9). 8. (8) Despite clause 4.5 of Schedule 1, an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have.
Disclosure to archives		
20 An organization may disclose personal information about an individual without the consent of the individual but only if one or more of the following are applicable: 20(p) the organization disclosing the information is an archival institution and the disclosure of the information is reasonable for archival purposes or research; 20(q) the disclosure of the information meets the requirements respecting archival purposes or research set out in the regulations and it is not reasonable to obtain the consent of the individual whom the information is about. *[see also PIPA Regulation sections 11-14]*	18(1) An organization may only disclose personal information about an individual without the consent of the individual, if 18(1)(n) the disclosure is to an archival institution if the collection of the personal information is reasonable for research or archival purposes,	7. (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is 7. (3)(g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;
11. Powers of Commissioner		
36(1) In addition to the Commissioner's powers and duties under Part 5 with respect to reviews, the Commissioner is	36(1) In addition to the commissioner's powers and duties under Part 11 with respect to reviews, the commissioner	

ALBERTA PIPA	BC PIPA	PIPEDA (Part 1)
generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may	is responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may do any of the following:	
36(1)(a) conduct investigations to ensure compliance with any provision of this Act;	36(1)(a) whether a complaint is received or not, initiate investigations and audits to ensure compliance with any provision of this Act, if the commissioner is satisfied there are reasonable grounds to believe that an organization is not complying with this Act;	11. (2) If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter. 18. (1) The Commissioner may, on reasonable notice and at any reasonable time, audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening a provision of Division 1 or is not following a recommendation set out in Schedule 1, and for that purpose may (a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary for the audit, in the same manner and to the same extent as a superior court of record; ... (d) at any reasonable time, enter any premises, other than a dwelling-house, occupied by the organization on satisfying any security requirements of the organization relating to the premises; ... (f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the audit
36(1)(f) comment on the implications for protection of personal information in relation to existing or proposed programs of organizations;	36(1)(f) comment on the implications for protection of personal information of programs proposed by organizations;	20. (2) The Commissioner may make public any information relating to the personal information management practices of an organization if the Commissioner considers that it is in the public interest to do so.
	36(1)(g) comment on the implications of automated systems for the protection of personal information;	
	36(1)(h) comment on the implications for protection of personal information of the use or disclosure of personal information held by organizations for document linkage	
38(2) The Commissioner may require any record to be produced to the Commissioner and may examine any information in a record, including personal information, whether or not the record is subject to this Act.	38(2) The commissioner may (a) examine any information in a document, including personal information, and obtain copies or extracts of documents containing information (i) found in any premises entered under paragraph (c), or (ii) provided under this Act, (b) require an individual or an organization to produce	12. (1)(a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record;

ALBERTA PIPA	BC PIPA	PIPEDA (Part 1)
	documents, and (c) at any reasonable time, enter any premises, other than a personal residence, occupied by an organization, after satisfying any reasonable security requirements of the organization relating to the premises.	(d) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises; (f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the investigation. [The Commissioner has the same powers when conducting an audit, see section 18]
52(2) If the inquiry relates to a decision of an organization to give or refuse to give access to all or part of the personal information about the individual or a record relating to the information, the Commissioner must, by order, do one of the following: (a) direct the organization to give the individual access to all or part of the personal information about the individual or any record relating to the information that is under the control of the organization if the Commissioner determines that the organization is not permitted under this Act to refuse access;	52(2) If the inquiry is into a decision of an organization to give or to refuse to give access to all or part of an individual's personal information, the commissioner must, by order, do one of the following: (a) require the organization (i) to give the individual access to all or part of his or her personal information under the control of the organization, (ii) to disclose to the individual the ways in which the personal information has been used, (iii) to disclose to the individual names of the individuals and organizations to whom the personal information has been disclosed by the organization, or (iv) if the organization is a credit reporting agency, to disclose to the individual the names of the sources from which it received personal information about the individual, if the commissioner determines that the organization is not authorized or required to refuse access by the individual to the personal information;	
12. Offences		
59(1) Subject to subsections (3) and (4), a person commits an offence if the person 59(1)(a) wilfully collects, uses or discloses personal information in contravention of Part 2;	56(1) Subject to subsection (2), an organization or person commits an offence if the organization or person (a) uses deception or coercion to collect personal information in contravention of this Act,	28. Every person who knowingly contravenes subsection 8(8) or 27.1(1) or who obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of (a) an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or (b) an indictable offence and liable to a fine not exceeding $100,000.
59(1)(b) wilfully attempts to gain or gains access to personal information in contravention of this Act;		
59(1)(c) disposes of or alters, falsifies, conceals or destroys personal information or any record relating to personal information, or directs another person to do so, with an intent to evade a request for access to the personal information or the record;	56(1)(b) disposes of personal information with an intent to evade a request for access to the personal information,	