AccessPrivacy Health Hub: Safeguarding Chart

Provincial health privacy statutes across Canada contain various requirements relating to the safeguarding of personal health information. The chart below details the specific safeguarding requirements under health privacy statutes in each province in Canada. Refer to the Safeguarding Health Sector Topic Hub for an overview of these statutory safeguarding requirements and related privacy regulatory authority guidance.

Jurisdiction	Safeguarding Measures
Ontario *Personal Health Information Protection Act*, 2004, S.O. 2004, c. 3, Sch. A; O. Reg. 329/04: GENERAL	**Definitions** **2 "information practices"**, in relation to a health information custodian, means the policy of the custodian for actions in relation to personal health information, including, […] (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information; **Information practices** **10** (1) A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this Act and its regulations. (2) A health information custodian shall comply with its information practices. **Security** **12** (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. **Written public statement** **16** (1) A health information custodian shall, in a manner that is practical in the circumstances, make available to the public a written statement that, (a) provides a general description of the custodian's information practices**;** *Regulations :* **6** (3) The following are prescribed as requirements with respect to a health information network provider in the course of providing services to enable a health information custodian to use electronic means to collect, use, disclose, retain or dispose of personal health information: […] 5. The provider shall perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to, i. threats, vulnerabilities and risks to the security and integrity of the personal health information, and

Jurisdiction	Safeguarding Measures
	ii. how the services may affect the privacy of the individuals who are the subject of the information **Guidance:** • Safeguarding Personal Health Information (Current) • Unauthorized Access (Current) • Frequently Asked Questions, Personal Health Information Protection Act (2015)
Alberta *Health Information Act*, R.S.A. 2000, c. H-5 Health Information Regulation, Alta. Reg. 70/2001	**Duty to protect health information** **60** (1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will (a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information, (b) protect the confidentiality of health information that is to be stored or used in a jurisdiction outside Alberta or that is to be disclosed by the custodian to a person in a jurisdiction outside Alberta and the privacy of the individuals who are the subjects of that information, (c) protect against any reasonably anticipated (i) threat or hazard to the security or integrity of the health information or of loss of the health information, or (ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information, and (d) otherwise ensure compliance with this Act by the custodian and its affiliates. (2) The safeguards to be maintained under subsection (1) must include appropriate measures (a) for the security and confidentiality of records, which measures must address the risks associated with electronic health records, and (b) for the proper disposal of records to prevent any reasonably anticipated unauthorized use or disclosure of the health information or unauthorized access to the health information following its disposal. **(3)** In subsection (2)(a), "electronic health records" means records of health information in electronic form. *Regulations:*

Jurisdiction	Safeguarding Measures
	8 (1) A custodian must identify, and maintain a written record of, all of its administrative, technical and physical safeguards in respect of health information. (2) A custodian must designate an individual who is responsible for the overall security and protection of health information in the custody or under the control of the custodian. (3) A custodian must periodically assess its administrative, technical and physical safeguards in respect of (a) the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information, (b) any reasonably anticipated threat or hazard to the security or integrity of the health information or to the loss of the health information, and (c) any unauthorized use, disclosure or modification of the health information or unauthorized access to the health information. (6) A custodian must ensure that its affiliates are aware of and adhere to all of the custodian's administrative, technical and physical safeguards in respect of health information. (7) A custodian must establish sanctions that may be imposed against affiliates who breach, or attempt to breach, the custodian's administrative, technical and physical safeguards in respect of health information. **Guidance:** • Responsibilities of Custodians and Health Information Act Administration Checklist (2011) • A Practical Guide to the Health Information Act (2010)
Saskatchewan *Health Information Protection Act*, S.S. 1999, c. H-0.021	**Duty to Protect** **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will: (a) protect the integrity, accuracy and confidentiality of the information; (b) protect against any reasonably anticipated: (i) threat or hazard to the security or integrity of the information;

Jurisdiction	Safeguarding Measures
	(ii) loss of the information; or (iii) unauthorized access to or use, disclosure or modification of the information; and (c) otherwise ensure compliance with this Act by its employees. **Guidance:** • IPC Guide to HIPA (2016)
Manitoba *The Personal Health Information Act*, C.C.S.M. c. P33.5 Personal Health Information Regulation, Man. Reg. 245/97	**Duty to adopt security safeguards** **18** (1) In accordance with any requirements of the regulations, a trustee shall protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information. (2) Without limiting subsection (1), a trustee shall (a) implement controls that limit the persons who may use personal health information maintained by the trustee to those specifically authorized by the trustee to do so; (b) implement controls to ensure that personal health information maintained by the trustee cannot be used unless (i) the identity of the person seeking to use the information is verified as a person the trustee has authorized to use it, and (ii) the proposed use is verified as being authorized under this Act; (c) if the trustee uses electronic means to request disclosure of personal health information or to respond to requests for disclosure, implement procedures to prevent the interception of the information by unauthorized persons; and (d) when responding to requests for disclosure of personal health information, ensure that the request contains sufficient detail to uniquely identify the individual the information is about. (3) A trustee who maintains personal health information in electronic form shall implement any additional safeguards for such information required by the regulations. **Safeguards for sensitive information** **19** In determining the reasonableness of security safeguards required under section 18, a trustee shall take into account the degree of sensitivity of the personal health information to be protected. *Regulations:* **3** A trustee shall (a) ensure that personal health information is maintained in a designated area or areas and is subject to appropriate security safeguards;

Jurisdiction	Safeguarding Measures
	(b) limit physical access to designated areas containing personal health information to authorized persons; (c) take reasonable precautions to protect personal health information from fire, theft, vandalism, deterioration, accidental destruction or loss and other hazards; and (d) ensure that removable media used to record personal health information is stored securely when not in use. **4**(1) In accordance with guidelines set by the minister, a trustee shall create and maintain, or have created and maintained, a record of user activity for any electronic information system it uses to maintain personal health information. *Regulations:* **8**(1) A trustee shall conduct an audit of its security safeguards at least every two years. (2) If an audit identifies deficiencies in the trustee's security safeguards, the trustee shall take steps to correct the deficiencies as soon as practicable. **Guidance:** • Frequently Asked Questions about PHIA (Current)
New Brunswick *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05	**Definitions** **1** "information practices" , in relation to a custodian, means the policy of the custodian governing actions in relation to personal health information, including (a) when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information, and (b) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information. **Security safeguards** **50** (1) In accordance with any requirements prescribed by the regulations, a custodian shall protect personal health information by adopting information practices that include reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information. (2) The information practices referred to in subsection (1) shall be based on nationally or jurisdictionally recognized information technology security standards and processes, appropriate for the level of sensitivity of the personal health information to be protected. (3) Without limiting subsection (1), a custodian shall (a) implement controls that limit the persons who may use personal health information maintained by the custodian to those specifically authorized by the custodian to do so,

Jurisdiction	Safeguarding Measures
	(b) implement controls to ensure that personal health information maintained by the custodian cannot be used unless (i) the identity of the person seeking to use the information is verified as a person the custodian has authorized to use it, and (ii) the proposed use is verified as being authorized under this Act, (c) if the custodian uses electronic means to request disclosure of personal health information or to respond to requests for disclosure, implement procedures to prevent the interception of the information by unauthorized persons, (d) when responding to requests for disclosure of personal health information, ensure that the request contains sufficient detail to uniquely identify the individual to whom the information relates, and (e) ensure agents of the custodian adhere to the safeguards. (4) A custodian who maintains personal health information in electronic form shall implement any additional safeguards for the security and protection of the information required by the regulations. **Guidance:** • Guidelines for Custodians – to assess compliance with the Personal Health Information Privacy and Access Act (PHIPAA) • Preparing for the Personal Health Information Privacy and Access Act (PHIPAA): A Checklist for Custodians • The Personal Health Information Privacy and Access Act (PHIPAA): Important Facts for Custodians
Nova Scotia *Personal Health Information Act*, SNS 2010, c 41 Personal Health Information Regulations, N.S. Reg 217/2012	**3** (n) "information practices", in relation to a custodian or a prescribed entity, means the policies of the custodian or a prescribed entity for actions in relation to personal health information, including (i) when, how and the purposes for which the custodian routinely collects, uses, discloses, retains, de-identifies, destroys or disposes of personal health information, and (ii) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information; **62** (1) A custodian shall implement, maintain and comply with information practices that (a) meet the requirements of this Act and the regulations; (b) are reasonable in the circumstances; and (c) ensure that personal health information in the custodian's custody or under its control is protected against

Jurisdiction	Safeguarding Measures
	(i) theft or loss of the information, and (ii) unauthorized access to or use, disclosure, copying or modification of the information. **65** A custodian who maintains an electronic information system shall implement any additional safeguards for such information required by the regulations. **68** A custodian shall, in a manner that is practical in the circumstances, make available to the public a written statement that (a) provides a general description of the custodian's information practices; *Regulations:* **10** (1) The following are prescribed as additional safeguards that a custodian must implement under Section 65 of the Act for personal health information held in an electronic information system maintained by the custodian: (a) protection of network infrastructure, including physical and wireless networks, to ensure secure access; (b) protection of hardware and its supporting operating systems to ensure that the system functions consistently and only those authorized to access the system have access; and (c) protection of the system's software, including the way it authenticates a user's identity before allowing access. (2) A custodian must create and maintain written policies to support and enforce the implementation of the safeguards required by subsection (1). **Guidance:** • Guide to Prince Edward Island Health Information Act (2017) • Frequently Asked Questions for Custodians: The Prince Edward Island Health Information Act (2017)
P.E.I. *Health Information Act, RSPEI 1988*, c H-1.41	**Protection of personal health information** **39** (1) A custodian shall protect personal health information by adopting information practices that include reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information. (2) The information practices referred to in subsection (1) shall be based on nationally or provincially recognized information technology and security standards and processes that are appropriate for the level of sensitivity of the personal health information to be protected. (3) The information practices referred to in subsection (1) shall include appropriate measures to address the risks associated with the storage of personal health information, taking into account the manner and form in which the personal health information is recorded, the location of storage and the degree of sensitivity of the personal health information to be protected. (4) Without limiting the generality of subsection (1), a custodian shall

Jurisdiction	Safeguarding Measures
	(a) implement controls that limit the persons who may use personal health information maintained by the custodian to those specifically authorized by the custodian to do so, including where appropriate the restriction of access to an individual's personal health information by an employee, agent, contractor or volunteer of the custodian or by a health care professional who has the right to treat persons at a health care facility operated by the custodian to only that personal health information that the employee, agent, contractor, volunteer or health care professional requires to carry out the purpose for which the personal health information was collected or will be used; (b) implement safeguards and controls to ensure that personal health information maintained by the custodian cannot be used unless (i) the identity of the person seeking to use the personal health information is verified as a person the custodian has authorized to use it, and (ii) the proposed use is verified as being authorized under this Act; (c) if the custodian uses electronic means to request disclosure of personal health information or to respond to requests for disclosure, implement procedures to prevent the interception of the personal health information by unauthorized persons; (d) provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information; (e) when responding to requests for disclosure of personal health information, ensure that the request contains sufficient detail to uniquely identify the individual to whom the information relates; and (f) ensure agents of the custodian adhere to the safeguards and controls implemented to protect personal health information. (5) This section does not override or modify any requirement in an enactment or an Act of the Parliament of Canada concerning the retention or secure destruction of records of personal health information maintained by a custodian.
Newfoundland and Labrador *Personal Health Information Act*, SNL 2008, c P-7.01 *Personal Health Information Regulations*, NLR 38/11	**Information practices, policies and procedures** **13** (1) A custodian that has custody or control of personal health information shall establish and implement information policies and procedures to facilitate the implementation of, and ensure compliance with, this Act and the regulations respecting the manner of collection, storage, transfer, copying, modification, use and disposition of personal information whether within or outside the province. (2) The information policies and procedures referred to in subsection (1) shall include policies and procedures to (a) protect the confidentiality of personal health information that is in its custody or under its control and the privacy of the individual who is the subject of that information;

Jurisdiction	Safeguarding Measures
	(b) restrict access to an individual's personal health information by an employee, agent, contractor or volunteer of the custodian or by a health care professional who has the right to treat persons at a health care facility operated by the custodian to only that information that the employee, agent, contractor, volunteer or health care professional requires to carry out the purpose for which the information was collected or will be used; (c) protect the confidentiality of personal health information that will be stored or used in a jurisdiction outside the province or that is to be disclosed by the custodian to a person in another jurisdiction and the privacy of the individual who is the subject of that information; and (d) provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information. **(3)** The information policies and procedures referred to in subsection (1) shall include appropriate measures to address the risks associated with the storage of personal health information, taking into account the manner and form in which the personal health information is recorded, the location of storage and the degree of sensitivity of the personal health information to be protected. **Obligations of employees, etc.** **14** (1) A custodian shall ensure that (a) its employees, agents, contractors and volunteers; and (b) where the custodian is an operator of a health care facility, those health care professionals who have the right to treat persons at a health care facility operated by the custodian, take an oath or affirmation of confidentiality. **Security** **15** (1) A custodian shall take steps that are reasonable in the circumstances to ensure that (a) personal health information in its custody or control is protected against theft, loss and unauthorized access, use or disclosure; (b) records containing personal health information in its custody or control are protected against unauthorized copying or modification; and (c) records containing personal health information in its custody or control are retained, transferred and disposed of in a secure manner. (2) For the purpose of paragraph (1)(c), "disposed of in a secure manner" in relation to the disposition of a record of personal health information does not include the destruction of a record unless the record is destroyed in such a manner that the reconstruction of the record is not reasonably foreseeable in the circumstances. **19** A custodian shall, in a manner that is practical in the circumstances, make available to those who are or who are likely to be affected by the custodian's activities a written statement that (a) provides a general description of the custodian's information policies and procedures; **Guidance:**

Jurisdiction	Safeguarding Measures
	• The Personal Health Information Act Frequently Asked Questions (2011)
Yukon *Health Information Privacy And Management Act*, SY 2013, c 16 *Health Information General Regulation*, YOIC 2016/159	**Custodian's information practices generally** **19** (1) A custodian must protect personal health information by applying information practices that include administrative policies and technical and physical safeguards that ensure the confidentiality, security, and integrity of the personal health information in its custody or control (2) The information practices referred to in subsection (1) must be based on the standards that are prescribed for this purpose. (3) Without limiting subsection (1), a custodian must, in relation to personal health information in its custody or control (a) implement measures that protect the confidentiality, privacy, integrity and security of personal health information and that prevent its unauthorized modification; (b) implement controls that limit the individuals who may use personal health information to those specifically authorized by the custodian to do so; (c) implement controls to ensure that personal health information cannot be used unless (i) the identity of the individual seeking to use the personal health information is verified as an individual the custodian has authorized to use it, and (ii) the proposed use is authorized under this Act; (d) take all reasonable steps to prevent a security breach; (e) provide for the secure storage, disposal and destruction of records to minimize the risk of unauthorized access to, or disclosure of, personal health information; (f) develop policies which provide that personal health information is retained in accordance with the prescribed requirements, if any; (g) establish a procedure for receiving and responding to complaints regarding its information practices; and (h) meet the prescribed requirements, if any. **Statement of information practices to be made public** **21** A custodian must make available to the public a written statement that (a) provides a general description of the custodian's information practices; **[…]** *Regulations:*

Jurisdiction	Safeguarding Measures
	Custodian's information practices **14** (1) For the purposes of section 19 of the Act, a custodian must in respect of personal health information that is in the custodian's custody and control (a) for each of the custodian's agents (i) determine the personal health information that the agent is authorized to access (ii) ensure that the agent signs a pledge of confidentiality that includes an acknowledgement that the agent is bound by the Act and is aware of the consequences of breaching it, and (iii) where appropriate, provide privacy and security orientation and ongoing training; (b) ensure that the custodian has, in writing (i) policies in relation to the collection, use and disclosure of personal health information (ii) policies on security breaches that describes how the custodian complies with Division 5 of Part 3 of the Act, and (iii) a policy in relation to individuals' access to and correction of their personal health information (c) at least every two years, conduct an audit of the custodian's security safeguards, including information practices and procedures (d) as soon as possible, identify and address any deficiencies identified in an audit conducted under paragraph (c); […] (f) ensure that personal health information is maintained in a designated area and is subject to appropriate security safeguards (g) limit physical access to designated areas containing personal health information to authorized persons; (h) ensure that a written record is created of all security breaches; and (i) address the privacy and security risks of an agent's remote access to the custodian's information systems, including through the use of the agent's own mobile electronic device **(2)** The information practices referred to in section 19 of the Act (including, for greater certainty, those described in this section) must be based on the standard of what is reasonable, taking into account the sensitivity of the personal health information

Jurisdiction	Safeguarding Measures
Northwest Territories *Health Information Act*, SNWT 2014, c 2 *Health Information Regulations*, NWT Reg 089-2015	**Measures for protection of information** **85** (1) A health information custodian shall take protection of information reasonable measures to maintain administrative, technical and physical safeguards for the protection of personal health information, including for protection (a) of the confidentiality of personal health information and the privacy of individuals the information is about; (b) of the confidentiality of personal health information that is to be stored or used outside the Northwest Territories, or that is to be disclosed by the custodian to a person or organization outside the Territories; (c) against unauthorized access to or unauthorized use, disclosure or alteration of personal health information; (d) against loss or unauthorized destruction or other disposal of personal health information; and (e) against theft or any other reasonably anticipated threat or hazard to the security or integrity of personal health information **Authorization of users** **(2)** A health information custodian shall implement controls that limit the persons who may use personal health information maintained by the custodian to those authorized to do so **Protection of records** **86. (1)** A health information custodian shall take reasonable measures to protect the security and confidentiality of records that contain personal health information, including measures to ensure that the records (a) are maintained in a secure manner; (b) are, if applicable, transferred in a secure manner; and (c) are, on destruction or other disposal, disposed of in a secure manner. **Electronic health records** **(2)** The measures under subsection (1) must include measures to address risks to confidentiality and privacy associated with electronic health records that are based on nationally or territorially recognized information technology security standards and processes that are appropriate for the high level of sensitivity of personal health information. *Regulations:* **Safeguards**

Jurisdiction	Safeguarding Measures
	13. (1) The administrative, technical and physical safeguards required under section 85 of the Act must include (a) measures to protect personal health information through an assessment of re-identification risk and the application of de-identification procedures as required; (b) measures to protect network infrastructure from interruption and unauthorized access and use; (c) the use of authentication and encryption to protect information stored electronically; (d) measures to prevent and respond to problems involving hardware and software that might threaten the security, confidentiality or integrity of personal health information; (e) measures to protect hardware and software from unauthorized access and use; (f) measures to protect personal health information stored and transported on removable media; (g) a requirement that personal health information be maintained in a designated area subject to appropriate security safeguards; (h) a requirement that access to personal health information be monitored on an ongoing basis for the purpose of ensuring that only authorized access is occurring; (i) procedures that provide for the recording, reporting and investigation of security and privacy breaches; and (j) procedures that provide for effective prevention of, response to and remediation of security and privacy breaches **(2)** For the purposes of section 85 of the Act, measures to maintain safeguards must be proportionate to any threat to the security, confidentiality or integrity of personal health information. *Regulations:* **Safeguards** **13** (1) The administrative, technical and physical safeguards required under section 85 of the Act must include (a) measures to protect personal health information through an assessment of re-identification risk and the application of de-identification procedures as required; […] (3) A health information custodian shall review its compliance with and the effectiveness of its administrative, technical and physical safeguards on an annual basis.