Dialogue

Contract Review Operating Guideline - Outsourcing

Version: 2
Date of last revision: August 1, 2024
Effective Date: August 1, 2024

CONFIDENTIAL

1. OBJECTIVE

1.1 Dialogue may use Personal Information and information technology systems in various aspects of its business.

1.2 Under Applicable Privacy Legislation, Dialogue is responsible for Personal Information in its custody or under its control, including Personal Information that has been transferred to a third-party Service Provider for Processing. As such, contracts with third-party Service Providers must provide guarantees of confidentiality and security of Personal Information.

1.3 This Operating Guideline provides guidance to Dialogue Agents for assessing and managing privacy risks with respect to the Processing of Personal Information by third-party Service Providers under outsourcing contracts currently in effect.

1.4 While Dialogue has implemented an Outsourcing Operating Guideline[1] to ensure that it complies with Applicable Privacy Legislation on a go forward basis, it must undertake the review of current outsourcing contracts to determine if they include the relevant data security language.

2. DEFINITIONS

2.1 Refer to Appendix A of the Internal Privacy Policy for the Glossary of Terms.

3. ROLES AND RESPONSIBILITIES

3.1 The Privacy Officer is responsible for the implementation and revision of this Operating Guideline.

3.2 Dialogue Agents are required to adhere to this Operating Guideline.

4. DETAILS

4.1 Step 1: Inventory of third-party Service Providers Processing Personal Information

4.1.1 The relevant Dialogue Agent must first prepare an inventory of **current third-party Service Providers** that may be Processing Personal Information in the custody of or under the control of Dialogue.

4.1.2 For each third-party Service Provider, the following information must be verified and captured in the Service Provider inventory:

4.1.2.1 Dialogue Agent responsible for relationship with the third-party Service Provider;

[1] These Operating Guidelines must be read together with the most current version of Dialogue's Data Protection Addendum (or "**DPA**").

4.1.2.2 Dialogue department in charge of relationship with third-party Service Provider;

4.1.2.3 Name of third-party Service Provider;

4.1.2.4 Description of the role of the third-party Service Provider;

4.1.2.5 Categories of individuals whose Personal Information is transferred to the third-party Service Provider;

4.1.2.6 Categories of Personal Information transferred to third-party Service Provider;

4.1.2.7 If applicable, countries outside Canada in which Personal Information is stored or accessed;

4.1.2.8 Existence of a written contract with third-party Service Provider;

4.1.2.9 If applicable, contract expiration/termination date, and automatic renewal period.

4.1.3 Once the inventory of third-party Service Providers has been prepared, the Dialogue Agent must comply with the following instructions:

4.1.3.1 If there is a contract in place, go to step 2 to determine if such contract includes sufficient data security / privacy protections.

4.1.3.2 If there is no contract in place, go directly to step 3.

4.2 Step 2: Review Contractual Privacy Protection Provisions

4.2.1 The Dialogue Agent must use this checklist to assess whether the agreement between Dialogue and a third-party Service Provider includes sufficient data security / privacy protections.

4.2.2 Checklist – Contractual privacy protections:

☐ **Compliance with data protection laws –** The third-party Service Provider must undertake to comply with Applicable Privacy Legislation.

☐ **Purpose limitation –** The third-party Service Provider may only Process Personal Information pursuant to the instructions of Dialogue and for the purposes of providing the services to Dialogue under the service agreement.

☐ **Transfers to third parties –** Transfers of Personal Information to third parties, including affiliates and sub-processors, are prohibited unless authorized by Dialogue. If a third-party Service Provider transfers Personal

Information to a third party, it must flow down the privacy obligations of the contract to that third party.

☐ **Data subject requests** – If a third-party Service Provider receives a request from an individual regarding their rights under Applicable Privacy Laws, such as access and rectification rights, they must inform Dialogue and collaborate with Dialogue to respond to the request.

☐ **Limitations on Access** – A third-party Service Provider must limit access to Personal Information to only those individuals that need access to deliver the services and have been appropriately trained about the third-party Service Provider's privacy and security obligations under the DPA and Applicable Privacy Legislation.

☐ **Security** – A third-party Service Provider must protect Personal Information with adequate administrative, technical and physical safeguards (see the "Security Program Minimum Requirements" in Schedule B of the DPA for details).

☐ **Privacy Incidents** – A third-party Service Provider must immediately notify Dialogue of any Privacy Incident impacting the Personal Information made available by Dialogue or accessed by the third-party Service Provider on behalf of Dialogue.

☐ **Security review and audit** – A third-party Service Provider must allow Dialogue to audit its data protection and security practices.

☐ **Secure disposition/destruction** –A third-party Service provider must securely return or dispose of all Personal Information upon the termination of the service agreement.

☐ **Cross-border transfers (Canada)** - Transfers of Personal Information of Canadian residents outside of Canada (or for outside a province, where such a transfer is restricted by Applicable Privacy Legislation) must be approved by Dialogue in writing.

4.2.3 If the contract in place already includes the necessary security provisions, the Dialogue Agent must go directly to step 5.

4.2.4 If the contract in place does not include the necessary security provisions, the Dialogue Agent must go to step 3.

4.3 Step 3: Preparing the Data Protection Addendum

4.3.1 The Dialogue Agent (with oversight from the Privacy Officer must follow the instructions detailed in this step 3 if:

4.3.1.1 there is no contract in place; or

4.3.1.2 the contract in place does not include the necessary security provisions (as evaluated under Step 2).

4.3.2 You must first finalize the DPA as follows:

4.3.3 On page 1 of the DPA, you must insert:

4.3.3.1 The full name of the legal entity contracting with the third-party Service Provider defined as "Company" if this entity is not Dialogue

4.3.3.2 The full name of the legal entity providing the services defined as "Service Provider".

4.3.3.3 If there is a written contract in place:

(a) include details on the type of service agreement in place before the definition of "Agreement" (such as the title and date of the said services agreement);

(b) include details on the type of services provided by the third-party Service Provider under the agreement, before the definition of "Services" (such as "cloud storage services", "payroll services", etc.).

4.3.3.4 If there is no contract in place, adjust the language and content of the DPA accordingly in order to reflect the existence of the verbal agreement.

4.3.4 On the last page of the DPA (before Schedule A), you must insert in the signature blocks:

4.3.4.1 The full name of the legal entity contracting with the third-party Service Provider if this entity is not Dialogue Health Technologies Inc.; and

4.3.4.2 The full name of the third-party Service Provider (i.e. legal entity providing the services).

4.3.5 In Schedule "A" of the DPA, you must insert the following information:

4.3.5.1 Details pertaining to the third-party Service Provider: name and contact details, Processing activities and location;

4.3.5.2 Details pertaining to the third-party Service Provider's sub-processors (if any): name and contact details, Processing activities and location;

4.3.5.3 The categories of individuals impacted, such as a Dialogue Member, dependant, Dialogue Agent; and

4.3.5.4 The categories of Personal Information transferred or accessed (i.e. such as name, address, age, personal identification number, credit card information, device information, online behavior, location tracking, etc).

4.3.6 With respect to Schedule "B" of the DPA, in case of Personal Health Information will be Processed in any way by the third-party Service Provider, review the Provincial Health Privacy Legislation requirements with the Privacy Officer and/or IT/Security team to ensure the requirements are met. For details on legal requirements regarding Personal Health Information, refer to Appendix A hereof.

4.3.7 Once the DPA is finalized, the Dialogue Agent must go to step 4.

4.4 Step 4: Transmission of DPA to Relevant Third-Party Service Provider

4.4.1 The Dialogue IT/Security team should identify the relevant contact for each third-party Service Provider and send the finalized DPA by email with the relevant cover email depending on the rationale indicated in the third-party Service Provider Inventory.

4.4.2 After sending the email and the DPA to the third-party Service Provider, the Dialogue IT/Security team should follow up with the contact to make sure that the request is not left unanswered. In the event that the third-party Service Provider requests certain changes to the DPA, you can review the drafting notes in the template DPA under each provision to determine the rationale of the provision and whether it can be modified at the request of the third-party Service Provider.

4.4.3 Once an executed version of the DPA is received from the third-party Service Provider, the Dialogue Agent must go to step 5.

4.5 Step 5: Complete the Third-Party Service Provider Inventory

4.5.1 If the contract in place already includes the necessary security provisions, the Dialogue Agent must update the third-party Service Provider inventory, accordingly.

4.5.2 For situations where there was no contract in place or such contract did not include the necessary security provisions, once the third-party Service Provider has executed the DPA transmitted following Step 4, update the third-party Service Provider inventory.

5. ENFORCEMENT

5.1 The Privacy Officer may audit at any time to ensure compliance with this Operating Guideline. Failure to report known violations of this Operating

Guideline to the Privacy Officer is considered a violation of this Operating Guideline.

5.2 Dialogue Agents who violate this Operating Guideline may be subject to appropriate disciplinary action up to and including termination or termination of contractual agreements, denial of access to information technology resources, and other actions as well as both civil and criminal penalties.

Version History:

Version Number	Effective Date	Revision Date	Approval
1	August 1, 2022	August 1, 2022	Nathalie Delisle, Chief Privacy Officer Dr. Marc Robin, Medical Director
2	August 1, 2024	August 1, 2024	Dominique Payette, Privacy Officer

APPENDIX A

Outsourcing Requirements - Provincial Health Privacy Legislation[2]

Legislation	Type of Requirement	Summary of Requirement
Alberta *Health Information Act* (AB HIA)		
60(1)(b) and s. 8 of Alta Reg 70/2001	Security safeguards; data sovereignty	A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will: (i) 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; (ii) 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; (iii) protect against any reasonably anticipated threats to the security or integrity of the information or unauthorized, use, disclosure or modification of the information; and (iv) otherwise ensure compliance with this Act by the custodian and its affiliates. The safeguards must include appropriate measures: (i) for the security and confidentiality of records, which measures must address the risks associated with electronic health records; and (ii) 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. With respect to the prescribed security obligations, Alta Reg 70/2001 s. 8 requires a custodian to: ● identify, and maintain a written record of, all of its administrative, technical and physical safeguards in respect of health information; ● 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; ● periodically assess its administrative, technical and physical safeguards in respect of: (i) 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; (ii) any reasonably anticipated threat or hazard to the security or integrity of the health information or to the loss of the health information; and (iii)

[2] British Columbia, Quebec and Nunavut do not have provincial personal health information laws.

Legislation	Type of Requirement	Summary of Requirement
		any unauthorized use, disclosure or modification of the health information or unauthorized access to the health information; ● in order to ensure the privacy and confidentiality of health information that is to be stored or used by a person in a jurisdiction outside Alberta or that is to be disclosed to a person in a jurisdiction outside Alberta, the custodian must, prior to the storage, use or disclosure of the information, enter into a written agreement with the person that: (i) provides for the custodian to retain control over the health information; (ii) adequately addresses the risks associated with the storage, use or disclosure of the health information; (iii) requires the person to implement and maintain adequate safeguards for the security and protection of the health information; (iv) allows the custodian to monitor compliance with the terms and conditions of the agreement; and (v) contains remedies to address any non-compliance with or breach of the terms and conditions of the agreement by the other person; ● 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; and ● 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.
64	PIA required for a change in administrative practices and information systems	Subject to subsection limited exceptions, each custodian must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information. The custodian must submit the privacy impact assessment to the Commissioner for review and comment before implementing any proposed new practice or system described above or any proposed change to existing practices and systems described above.
24, 43; 60	Obligations with respect to "affiliates" (third-party service providers)	An "affiliate" means, in relation to a custodian, (i) an individual employed by the custodian; (ii) a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian; (iii) a health services provider who is exercising the right to admit

Legislation	Type of Requirement	Summary of Requirement
		and treat patients at a hospital as defined in the *Hospitals Act*; (iv) an information manager; and (v) any person designated under the regulations. An affiliate of a custodian must not collect health information in any manner that is not in accordance with the affiliate's duties to the custodian. An affiliate of a custodian must not disclose health information in any manner that is not in accordance with the affiliate's duties to the custodian. Subject to the regulations, an affiliate of a custodian must as soon as practicable notify the custodian in accordance with the regulations of any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian.
66 and Alta Reg 70/2001 s. 7.2	Obligations with respect to information managers	An "information manager" means a person or body that: (i) processes, stores, retrieves or disposes of health information; (ii) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, or (iii) provides information management or information technology services in a manner that requires the use of health information, but does not include an individual employed by a custodian who performs any of the functions listed in clauses (i) to (iii). A custodian must enter into a written agreement with an information manager in accordance with the regulations for the provision of any or all of the services described above. Section 7.2 of Alta Reg 70/2001 requires the written agreement to: ● identify the objectives of the agreement and the principles to guide the agreement; ● indicate whether or not the information manager is permitted to collect health information from any other custodian or from a person and, if so, describe that health information and the purpose for which it may be collected; ● indicate whether or not the information manager may use health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be used;

Legislation	Type of Requirement	Summary of Requirement
		• indicate whether or not the information manager may disclose health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be disclosed; • describe the process for the information manager to respond to access requests under Part 2 of the Act or, if the information manager is not to respond to access requests, describe the process for referring access requests for health information to the custodian itself; • describe the process for the information manager to respond to requests to amend or correct health information under Part 2 of the Act or, if the information manager is not to respond to requests to amend or correct health information, describe the process for referring access requests to amend or correct health information to the custodian itself; • describe how health information provided to the information manager is to be protected, managed, returned or destroyed in accordance with the Act; • describe how the information manager is to address an expressed wish of an individual relating to the disclosure of that individual's health information or, if the information manager is not to address an expressed wish of an individual relating to the disclosure of that individual's health information, describe the process for referring these requests to the custodian itself; and • set out how an agreement can be terminated. A custodian that has entered into an agreement with an information manager may provide health information to the information manager without the consent of the individuals who are the subjects of the information for the purposes authorized by the agreement, provided that an information manager to which information is provided may use or disclose that information only for the purposes authorized by the agreement. An information manager must comply with (i) the *Health Information Act* and its regulations; and (ii) the agreement entered into with a custodian in respect of information provided to it. A custodian continues to be responsible for compliance with *Health Information Act* and its regulations in respect of the information provided by the custodian to the information manager.

Legislation	Type of Requirement	Summary of Requirement
Saskatchewan *Health Information Protection Act*		
16	Security safeguards	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: (i) protect the integrity, accuracy and confidentiality of the information; (ii) protect against any privacy breach; and (iii) otherwise ensure compliance with this Act by its employees.
18(1)	Obligations with respect to information management service providers	An "information management service provider" means a person who or body that processes, stores, archives or destroys records of a trustee containing personal health information or that provides information management or information technology services to a trustee with respect to records of the trustee containing personal health information, and includes a trustee that carries out any of those activities on behalf of another trustee, but does not include a trustee that carries out any of those activities on its own behalf. A trustee may provide personal health information to an information management service provider: (i) for the purpose of having the information management service provider process, store, archive or destroy the personal health information for the trustee; (ii) to enable the information management service provider to provide the trustee with information management or information technology services; (iii) for the purpose of having the information management service provider take custody and control of the personal health information pursuant to section 22 when the trustee ceases to be a trustee; and (iv) for the purpose of combining records containing personal health information. An information management service provider shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out above. If a trustee is also an information management service provider and has received personal health information from another trustee in accordance with subsection (1), the trustee receiving the information is deemed to be an information management service provider for the purposes of that personal health information and does not have any of the rights and duties of a trustee with respect to that information.

Legislation	Type of Requirement	Summary of Requirement
Manitoba *Personal Health Information Act*		
18-19; Man Reg 245/97 ss. 2-4	Security safeguards	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. Man Reg 245/97 Sections 2-3 further require a trustee to: ● maintain a written policy and procedures addressing the security of personal health information, security breaches and corrective procedures to address security breaches; and ● adopt the following physical security safeguards: (i) ensuring personal health information is maintained in a designated area; (ii) limiting physical access to those designated areas; (iii) adopting precautions to protect personal health information against fire, theft, vandalism, deterioration, accidental destruction and other hazards; and (iv) securely storing removable media used to record personal health information. Without limiting the foregoing, a trustee must: ● 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; ● 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; ● 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 ● 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.

Legislation	Type of Requirement	Summary of Requirement
		A trustee who maintains personal health information in electronic form shall implement any additional safeguards for such information required by the regulations. Man Reg 245/97 requires a trustee to adopt the following: ● a record of user activity for the system that must be maintained for at least three years; and ● regular audits of user activity to detect security breaches. In determining the reasonableness of security safeguards required above, a trustee shall take into account the degree of sensitivity of the personal health information to be protected.
25	Requirements with respect to providing information to information management service providers	An "information manager" means a person or body that: (i) processes, stores or destroys personal health information for a trustee; or (ii) provides information management or information technology services to a trustee. A trustee may provide personal health information to an information manager for the purpose of processing, storing or destroying it or providing the trustee with information management or information technology services. An information manager may use personal health information provided to it under this section only for the purposes and activities mentioned above, which must be purposes and activities that the trustee itself may undertake. A trustee who wishes to provide personal health information to an information manager under this section must enter into a written agreement with the information manager that provides for the protection of the personal health information against such risks as unauthorized access, use, disclosure, destruction or alteration, in accordance with the regulations. An information manager shall comply with: (i) the same requirements concerning the protection, retention and destruction of personal health information that the trustee is required to comply with under this Act; and (ii) the duties imposed on the information manager under the agreement described above. Personal health information that has been provided to an information manager under an agreement described in subsection (3) is deemed to be maintained by the trustee for the purposes of this Act.
Ontario *Personal Health Information Protection Act*		

Legislation	Type of Requirement	Summary of Requirement
10(4); O Reg 329/04 s. 6(1)	Obligations with respect to electronic systems service providers	A person who provides goods or services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with the prescribed requirements, if any. O Reg 329/04 requires such person to: ● not use any personal health information to which it has access in the course of providing the services for the health information custodian except as necessary in the course of providing the services; ● not disclose any personal health information to which it has access in the course of providing the services for the health information custodian; and ● not permit its employees or any person acting on its behalf to be able to have access to the information unless the employee or person acting on its behalf agrees to comply with the restrictions that apply to the person.
O Reg 329/04 s. 6(2)-(3)	Obligations with respect to health information network providers	A "health information network provider" or "provider" means a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians. A health information network provider is required to: ● notify every applicable health information custodian at the first reasonable opportunity if the provider accessed, used, disclosed or disposed of personal health information other than as necessary in the course of providing the services or an unauthorized person accessed the personal health information; ● provide to each applicable health information custodian a plain language description of the services that the provider provides to the custodians, that is appropriate for sharing with the individuals to whom the personal health information relates, including a general description of the safeguards in

Legislation	Type of Requirement	Summary of Requirement
		place to protect against unauthorized use and disclosure, and to protect the integrity of the information; ● make available to the public: (i) the plain language description described above; (ii) any directives, guidelines and policies of the provider that apply to the services that the provider provides to the health information custodians to the extent that these do not reveal a trade secret or confidential scientific, technical, commercial or labour relations information; and (iii) a general description of the safeguards implemented by the person in relation to the security and confidentiality of the information; ● to the extent reasonably practical and in a reasonably practical manner, keep and make available to each applicable health information custodian, on the request of the custodian, an electronic record of all access to and transfers of personal health information held in equipment controlled by the provider; ● 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 (ii) how the services may affect the privacy of the individuals who are the subject of the information; ● ensure that any third party it retains to assist in providing services to a health information custodian agrees to comply with the restrictions and conditions that are necessary to enable the provider to comply with this section; and ● enter into a written agreement with each health information custodian concerning the services provided to the custodian that: (i) describes the services that the provider is required to provide for the custodian; (ii) describes the administrative, technical and physical safeguards relating to the confidentiality and security of the information; and (iii) requires the provider to comply with the Act and its regulations.

Legislation	Type of Requirement	Summary of Requirement
12	Security safeguards	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.
17	Obligations with respect to agents	An "agent" means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated A health information custodian is responsible for personal health information in the custody or control of the health information custodian and may permit the custodian's agents to collect, use, disclose, retain or dispose of personal health information on the custodian's behalf only if: (i) the custodian is permitted or required to collect, use, disclose, retain or dispose of the information, as the case may be; (ii) the collection, use, disclosure, retention or disposal of the information, as the case may be, is necessary in the course of the agent's duties and is not contrary to this Act or another law; and (iii) prescribed requirements are met [none are currently prescribed]. A health information custodian may impose conditions or restrictions on an agent's ability to collect, use, disclose, retain or dispose of personal health information on the custodian's behalf. An agent may only collect, use, disclose, retain or dispose of personal health information on a custodian's behalf only if the collection, use, disclosure, retention or disposal of the information, as the case may be, is: (i) permitted by the custodian; (ii) necessary for the purpose of carrying out the agent's duties; (iii) not contrary to this Act or any other law; and (iv) complies with all conditions or restrictions imposed on the agent by the custodian. A health information custodian shall (i) take steps that are reasonable in the circumstances to ensure that no agent of the custodian collects, uses, discloses, retains or disposes of personal health information unless it is in accordance with the above; and (ii) remain responsible for any personal health information that is collected, used, disclosed, retained or disposed of by the custodian's agents, regardless of whether or not the collection, use, disclosure, retention or disposal was carried out in accordance with the above.

Legislation	Type of Requirement	Summary of Requirement
		An agent shall: (i) comply with the conditions or restrictions imposed by the health information custodian on the agent's collection, use, disclosure, retention or disposal of personal health information; and (ii) notify the custodian at the first reasonable opportunity if personal health information that the agent collected, used, disclosed, retained or disposed of on behalf of the custodian is stolen or lost or if it is used or disclosed without authority.
New Brunswick *Personal Health Information Privacy and Access Act*		
40	Security safeguards	A custodian must adopt reasonable administrative, technical and physical safeguards to ensure the confidentiality, security, accuracy and integrity of information that are based on nationally or jurisdictionally recognized information technology security standards and processes and are appropriate for the level of sensitivity of the personal health information to be protected. Without limiting the foregoing, a custodian must: ● 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; ● implement controls to ensure that personal health information maintained by the custodian cannot be used unless the identity of the person seeking to use the information is verified as a person the custodian has authorized to use it and the proposed use is verified as being authorized under this Act; ● 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; ● 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 ● ensure agents of the custodian adhere to the safeguards.

Legislation	Type of Requirement	Summary of Requirement
52(1)	Obligations with respect to agents	An "agent" means, in relation to a custodian, means an information manager or an individual or organization that acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian and not for the agent's own purposes, whether or not the information manager, individual or organization is remunerated by the custodian, but does not include an employee of the custodian. A custodian that retains the services of an agent for the collection, use, disclosure or retention of personal health information shall enter into a written agreement with the agent requiring the agent to comply with the custodian's legal obligations regarding handling of personal health information.
52(2)-(4)	Obligations with respect to information managers	An "information manager" means an individual or organization that on behalf of a custodian: (i) processes, stores, retrieves, archives or disposes of personal health information; (ii) de-identifies or otherwise transforms personal health information; or (iii) provides information management or information technology services. A custodian may provide personal health information to an information manager for the purpose of processing, storing or destroying the personal health information or providing the custodian with information management or information technology services. A custodian that wishes to provide personal health information to an information manager shall enter into a written agreement with the information manager, in accordance with the regulations, that provides for the protection of the personal health information against risks such as unauthorized access to or use or disclosure, secure destruction or alteration of the information. NB Reg 2010-112 s. 21 requires the written agreement to describe: ● the services provided to the custodian; and ● the administrative, technical and physical safeguards employed by the information manager relating to the confidentiality, security, accuracy and integrity of the personal health information. An information manager who enters into a written agreement described above shall comply with: (i) the duties imposed on the information manager under the agreement, and (ii) the same requirements

Legislation	Type of Requirement	Summary of Requirement
		concerning the protection, retention and secure destruction of personal health information that the custodian is required to comply with under this Act.
Newfoundland *Personal Health Information Act*		
13	Security safeguards	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, including policies and procedures to: ● 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; ● 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; ● 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 ● provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information. The information policies and procedures referred to above 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.

Legislation	Type of Requirement	Summary of Requirement
14	Obligations with respect to agents	An "agent" means, in relation to a custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's purposes, whether or not the agent has the authority to bind the custodian, is paid by the custodian or is being remunerated by the custodian. A custodian shall ensure its agents take an oath or affirmation of confidentiality. A custodian's agents shall comply with: (i) this Act and the regulations; and (ii) the information policies and procedures described above. A custodian shall ensure that its agents are aware of the duties imposed by this Act and the regulations and the information policies and procedures described above. A person who provides goods or services for the purpose of enabling a custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with this Act and the regulations
22	Obligations with respect to information managers	"Information manager" means a person or body, other than an employee of a custodian acting in the course of his or her employment, that: (i) processes, retrieves, stores or disposes of personal health information for a custodian; or (ii) provides information management or information technology services to a custodian. A custodian that retains the services of an information manager shall enter into an agreement with the information manager. The agreement shall be in writing and shall provide for the protection of the personal health information against unauthorized access, use, disclosure, disposition, loss or modification in accordance with this Act and the regulation.

Legislation	Type of Requirement	Summary of Requirement
		An information manager to which personal health information is disclosed by the custodian may use or disclose that information only for the purpose authorized by the agreement. An information manager shall comply with this Act and the regulations; and the terms of the agreement entered into with the custodian. An information manager shall not permit its employee or a person acting on its behalf to access the personal health information disclosed to it by the custodian unless the employee or person acting on its behalf agrees in writing to comply with this Act and the restrictions imposed upon the information manager referred to above. Nothing above relieves a custodian from its obligations under this Act and the regulations in respect of the personal health information disclosed by the custodian to the information manager, and the personal health information that has been disclosed to an information manager under an agreement is considered to continue in the custody and control of the custodian for the purpose of this Act and the regulations. An information manager may, in accordance with the terms of an agreement with a custodian, construct or create an integrated electronic record of personal health information comprising individual records, the custody or control of each of which may be in one or more custodians.
Prince Edward Island *Health Information Act*		
23	Disclosure permitted to information manager	A custodian may disclose personal health information relating to an individual without the consent of the individual if the disclosure is to an information manager in accordance with this Act;
25	PIA requirements	A custodian shall prepare a privacy impact assessment and submit the assessment to the Commissioner for review and comment in the following situations: ● for the new collection, use or disclosure of personal health information or any significant change to the collection, use or disclosure of personal health information;

Legislation	Type of Requirement	Summary of Requirement
		• for the creation of a personal health information system or personal health information communication technology or a significant modification to a personal health information system or personal health information communication technology; or • if a custodian performs data matching with personal health information collected by it or with any personal health information held by another custodian or another person.
39	Security safeguards	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. The information practices 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, and 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. Without limiting the foregoing, a custodian shall: • 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; • 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.

Legislation	Type of Requirement	Summary of Requirement
		• 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; • provide for the secure storage, retention and disposal of records to minimize the risk of unauthorized access to or disclosure of personal health information; • 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 • ensure agents of the custodian adhere to the safeguards and controls implemented to protect personal health information.
41	Obligations with respect to agents	An "agent" means in relation to a custodian, means a person that, with the authorization of the custodian, acts on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's purposes, whether or not the agent has the authority to bind the custodian, is paid by the custodian or is being remunerated by the custodian, and includes, but is not limited to, an employee of a custodian or a volunteer who deals with personal health information, a custodian's insurer, a lawyer retained by a custodian's insurer or a liability protection provider. A custodian that retains the services of an agent for the collection, use, disclosure, retention or secure destruction of personal health information shall enter into a written agreement with the agent requiring the agent to comply with: (i) the duties imposed on the agent under the agreement; and (ii) the same requirements concerning the protection, retention and secure destruction of personal health information that the custodian is required to comply with under this Act.
42-43	Obligations with respect to information managers	An "information manager" means a person or organization that on behalf of a custodian: (i) possesses, stores, retrieves, archives or disposes of personal health information; (ii) de-identifies or otherwise transforms personal health information; and (iii) provides information management or information technology services. A custodian may provide personal health information to an information manager for the purpose of processing, storing or destroying the personal health information or providing the custodian with

Legislation	Type of Requirement	Summary of Requirement
		information management or information technology services. A custodian that proposes to provide personal health information to an information manager shall enter into a written agreement with the information manager that provides for the protection of the personal health information against risks such as unauthorized access to or use or disclosure, secure destruction or alteration of the personal health information. An information manager who enters into a written agreement shall comply with: (i) the duties imposed on the information manager under the agreement; and (ii) the same requirements concerning the protection, retention and secure destruction of personal health information that the custodian is required to comply with under this Act.
Nova Scotia *Personal Health Information Act*		
28-29	Obligations with respect to agents	An "agent" means in relation to a custodian, means a person who, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's purposes, whether or not the agent has the authority to bind the custodian, is paid by the custodian or is being remunerated by the custodian, and includes, but is not limited to, an employee of a custodian or a volunteer who deals with personal health information, a custodian's insurer, a lawyer retained by the custodian's insurer or a liability protection provider. A custodian is responsible for personal health information in the custody or control of the custodian and may permit the custodian's agent to collect, use, disclose, retain, destroy or dispose of personal health information on the custodian's behalf only if: (i) the custodian is permitted or required to collect, use, disclose, retain, destroy or dispose of the information, as the case may be; (ii) the collection, use, disclosure, retention, destruction or disposition of the information, as the case may be, is in the course of the agent's duties and not contrary to the limits imposed by the custodian, this Act or another law; and (iii) the prescribed requirements are met, if any. Except as permitted or required by law and subject to the exceptions and additional requirements, if any, that are prescribed, an agent of a custodian shall not collect, use, disclose, retain, destroy or dispose of personal health information on the custodian's behalf unless the custodian permits the agent to do so.

Legislation	Type of Requirement	Summary of Requirement
		An agent of a custodian shall notify the custodian at the first reasonable opportunity if personal health information handled by the agent on behalf of the custodian is stolen, lost or accessed by unauthorized persons. Where a custodian is authorized to use personal health information for a purpose, the custodian may provide the information to an agent who may use it for that purpose on behalf of the custodian. For the purpose of this Act, the providing of personal health information between a custodian and an agent of the custodian is a use by the custodian, and not a disclosure by the custodian or a collection by the agent.
62	Security safeguards	A custodian shall implement, maintain and comply with information practices that: (i) meet the requirements of this Act and the regulations; (ii) are reasonable in the circumstances; and (iii) ensure that personal health information in the custodian's custody or under its control is protected against theft or loss of the information and unauthorized access to or use, disclosure, copying or modification of the information.
Yukon *Health Information Privacy and Management Act*		
19; YOIC 2016/159 s. 14	Security safeguards	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. The information practices referred to above must be based on the standards that are prescribed for this purpose. Without limiting the foregoing, a custodian must: ● implement measures that protect the confidentiality, privacy, integrity and security of personal health information and that prevent its unauthorized modification; ● implement controls that limit the individuals who may use personal health information to those specifically authorized by the custodian to do so;

Legislation	Type of Requirement	Summary of Requirement
		● 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; ● take all reasonable steps to prevent a security breach; ● provide for the secure storage, disposal and destruction of records to minimize the risk of unauthorized access to, or disclosure of, personal health information; ● develop policies which provide that personal health information is retained in accordance with the prescribed requirements, if any; ● establish a procedure for receiving and responding to complaints regarding its information practices; and ● meet the prescribed requirements, if any. YOIC 2016/159 s. 14 further requires that, for personal health information that is under the custodian's custody or control: ● for each of its agents: (i) determine the personal health information that the agent is authorized to access; (ii) ensure 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; ● ensure the custodian has, in writing, policies in relation to the collection, use and disclosure of personal health information; a policy on security breaches; and a policy in relation to access and correction requests; ● at least every two years, conduct an audit of the custodian's security safeguards, including their information practices and procedures; ● as soon as possible, identify and address any deficiencies identified in an audit conducted;

Legislation	Type of Requirement	Summary of Requirement
		● ensure that removable media used to record, transport or transfer personal health information are appropriately protected when in use and stored securely when not in use; ● ensure that personal health information is maintained in a designated area and is subject to appropriate security safeguards; ● limit physical access to designated areas containing personal health information to authorized persons; ● ensure that a written record is created of all security breaches; ● address the privacy and security risks of an agent's remote access to the custodian's information system, including through the use of the agent's own mobile electronic communication device.
49-50	Obligations with respect to agents	An "agent" means a person (other than a person who is prescribed not to be an agent of the custodian) who acts for or on behalf of the custodian in respect of personal health information, including for greater certainty such a person who is: (i) an employee of the custodian; (ii) a person who performs a service for the custodian under a contract or agency relationship with the custodian; (iii) an appointee, volunteer or student; (iv) an insurer or liability protection provider; (v) an information manager; (vi) if the custodian is a corporation, an officer or director of the corporation; and (vii) a prescribed person [none yet prescribed]. A custodian must take reasonable measures to ensure that its agents comply with this Act and the regulations. A custodian may permit its agent to collect, use, disclose, retain, destroy or dispose of personal health information on the custodian's behalf only if: (i) the custodian is permitted or required to collect, use, disclose, retain, destroy or dispose of the information, as the case may be; (ii) the collection, use, disclosure, retention, destruction or disposition of the information, as the case may be, is in the course of the agent's duties and is not contrary to the limits imposed by the custodian, this Act or any other enactment; (iii) the custodian allows the agent to use only that personal health information that the agent needs in order to carry out the purpose for which it was collected or a purpose for which use is authorized under this Act; and (iv) the prescribed requirements, if any, are met [none yet prescribed].

Legislation	Type of Requirement	Summary of Requirement
		Except as permitted or required by law, an agent of a custodian must not collect, use, disclose, retain, destroy or dispose of personal health information on the custodian's behalf unless the custodian permits the agent to do so. An agent of a custodian must notify the custodian at the first reasonable opportunity if a security breach has occurred in relation to any personal health information handled by the agent.
51; YOIC 2016/159 s. 21	Obligations with respect to information managers	An "information manager" means a person (other than a person who is prescribed not to be an information manager) who, for or on behalf of a custodian (i) processes, stores, retrieves, archives or disposes of information; (ii) strips, encodes or otherwise transforms identifying information to create information that is not identifying information; (iii) provides information management or information technology services; or (iv) provides a prescribed service [none yet prescribed]. A custodian who proposes to retain the services of an information manager must: (i) enter into a written agreement with the information manager that provides for the protection of the information that is the subject of the services; and (ii) comply with the prescribed requirements, if any. YOIC 2016/159 s. 21 requires that, when entering into a written agreement with an information manager in respect of personal health information under section 51 of the Act, a custodian must: ● ensure that the agreement allows the custodian to maintain control of the personal health information; and ● ensure that the agreement contains provisions which: o identify the objectives of the agreement and the principles that guide the agreement, o describe the types or classes of personal health information (referred to in this section as the "relevant personal health information") that the information manager may collect, use or disclose under the agreement, the purposes for which it may be collected, used or disclosed and any limitations or conditions on its collection, use or disclosure, o require the information manager: (i) to allow the custodian to access or otherwise obtain the relevant personal health information at any time, subject only to necessary operational constraints; (ii) to forward immediately to the custodian any access or correction request

Legislation	Type of Requirement	Summary of Requirement
		that is made in relation to the relevant personal health information; (iii) to maintain administrative, technical and physical safeguards that meet or exceed the safeguards required of the custodian under the Act to ensure the confidentiality, security and integrity of the relevant personal health information, and (iv) to inform the custodian promptly of the information manager's receipt of any requirement issued in a proceeding, including any summons, warrant or order, that relates to the relevant personal health information and that it is reasonable to believe may be enforceable in the jurisdiction in which the information manager operates or in which the relevant personal health information is located; o prohibit the information manager from subcontracting, without the custodian's written consent, any of the services to which the agreement relates; o allow the custodian to monitor and verify compliance with the agreement by the information manager; o allow the custodian to terminate the agreement in the event of a breach of the agreement by the information manager; and o set out that on termination of the agreement the personal health information to which the agreement applies must be transferred to the custodian, in an electronic format that the custodian can readily use, while ensuring ongoing access to the personal health information by the custodian, and requiring the information manager to cooperate fully with the custodian during the transfer, and following completion of the transfer, the information manager must securely destroy all records of the personal health information to which the agreement applies that remain in its custody. An information manager who enters into a written agreement must: (i) comply with the duties imposed on the information manager under the agreement and the prescribed requirements, if any; and (ii) notify the custodian at the first reasonable opportunity of any breach of the agreement by the information manager.

Legislation	Type of Requirement	Summary of Requirement
		[Note: It is not clear from the Act whether a transfer of personal health information to an information manager would constitute a "use" or a "disclosure". The Act does not contain any express permission to "disclose" to an information manager.]
Northwest Territories *Health Information Act*		
9-11	Obligations with respect to agents	An "agent" means a person or organization authorized to act as an agent that is: (i) an employee of the custodian; (ii) a person who performs a service for the custodian as an appointee, volunteer, student or under a contract or agency relationship; (iii) an information manager for the custodian; or (iv) a prescribed person. An agent shall not collect, use, disclose, manage, retain or dispose of personal health information in the course of the exercise of powers or the performance of duties or functions for a health information custodian unless authorized; or collect, use, disclose, manage, retain or dispose of personal health information contrary to any limits imposed by the custodian. An agent shall comply with this Act and the regulations. A health information custodian shall take reasonable measures to ensure that its agents comply with this Act and the regulations. An agent shall comply with standards, policies and procedures established or adopted by a health information custodian for purposes of implementing the requirements of this Act and the regulation. A health information custodian shall take reasonable measures to ensure that its agents comply with such standards, policies and procedures.
13	Obligations with respect to information managers	An "information manager" means a person or organization that provides one or more of the following services for a health information custodian: (i) the processing, storage, retrieval or disposal of personal health information; (ii) the transforming of personal health information, including the transforming of personal health information to create or produce non-identifying information; or (iii) information management services, information system services or information technology services. An "information management agreement" means an agreement in writing in respect of the protection of personal health information and privacy of individuals the information is about.

Legislation	Type of Requirement	Summary of Requirement
		Subject to limited exceptions, before using the services of an information manager, a health information custodian shall enter into an information management agreement with the information manager. The information management agreement must contain terms under which the information manager agrees to comply with: (i) this Act and the regulations, and standards, policies and procedures established or adopted by the health information custodian; (ii) measures to maintain administrative, technical and physical safeguards for the protection of the personal health information; and (iii) any other terms or conditions of the agreement. A health information custodian that has entered into an information management agreement under subsection may disclose personal health information to the information manager in accordance with the agreement. For greater certainty, a health information custodian may have more than one information manager and may, subject to the exceptions set out in this Act or the regulations, disclose personal health information to each information manager without the consent of the individuals the information is about. An information manager to which personal health information is disclosed shall not: (i) collect, use or disclose that information except in accordance with the information management agreement; or (ii) contravene the terms of an information management agreement.
85-86	Security safeguards	A health information custodian shall impose administrative, technical and physical safeguards over personal health information under its custody or control, including: ● measures to protect personal health information through an assessment of re-identification risk and the application of de-identification procedures as required; ● measures to protect network infrastructure from interruption and unauthorized access and use; ● the use of authentication and encryption to protect information stored electronically; ● measures to prevent and respond to problems involving hardware and software that might threaten the security, confidentiality or integrity of personal health information; ● measures to protect hardware and software from unauthorized access and use;

Legislation	Type of Requirement	Summary of Requirement
		• measures to protect personal health information stored and transported on removable media; • a requirement that personal health information be maintained in a designated area subject to appropriate security safeguards; • 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; • procedures that provide for the recording, reporting and investigation of security and privacy breaches; and • procedures that provide for effective prevention of, response to and remediation of security and privacy breaches. 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: (i) are maintained in a secure manner; (ii) are, if applicable, transferred in a secure manner; and (iii) are, on destruction or other disposal, disposed of in a secure manner. The measures described above 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. A health information custodian shall take measures to maintain records in an orderly records manner and to maintain an organized system of record-keeping, to ensure ease of access to the records when personal health information is required.