OVERVIEW OF KEY STATUTORY REQUIREMENTS APPLICABLE TO TRANSBORDER SERVICE PROVIDER ARRANGEMENTS

The following tables set out requirements and restrictions on transborder service provider arrangements under Canadian (i) provincial health sector privacy legislation (and, where applicable, public sector privacy legislation), and (ii) federal and provincial private sector privacy legislation.

With respect to transborder service provider arrangements (which include transfers to an affiliate acting as a service provider), there are generally no prohibitions on such arrangements under Canadian privacy laws. However, certain provinces/territories prescribe consent requirements, jurisdictional assessments and/or other safeguarding obligations where the service provider arrangement involves the transborder flow of personal information (which, for clarity, would include remote access by service providers located outside of Canada). In addition to the prescribed requirements set out below, in order to meet accountability and safeguarding obligations under Canadian privacy laws across all jurisdictions, accountable organizations should take steps to ensure (e.g., by conducting diligence on the service provider and assessing the geopolitical environment, national security laws and privacy regime in effect in the jurisdiction in question) that personal information will receive adequate protection (having regard to the sensitivity of the information) when transferred to or accessed in another jurisdiction.

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
Ontario[1] Information and Privacy Commissioner of Ontario *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A ("Ontario PHIPA") *General*, O Reg 329/04 ("Ontario Regulation")	None.[2]
British Columbia	Yes, under BC FIPPA for "public bodies".

[1] For the purpose of this chart, we have **not** included provisions applicable to agreements with health information network providers under Ontario PHIPA. A health information network 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 (s. 6(2), Ontario Regulation).

[2] Although Ontario PHIPA contains provisions relating to disclosures outside Ontario (s. 50), "the providing of personal health information between a health information custodian and an agent of the custodian is a use by the custodian, and not a disclosure by the person providing the information or a collection by the person to whom the information is provided." (s. 6(1), Ontario PHIPA).

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
Office of the Information and Privacy Commissioner for British Columbia ("OIPC BC") *Personal Information Protection Act*, SBC 2003, c. 63 ("BC PIPA") *Personal Information Protection Act Regulations*, B.C. Reg. 473/2003 *Freedom of Information and Protection of Privacy Act* ("BC FIPPA") *B.C. Reg. 155/2012* ("BC FIPPA Regulation") *B.C. Reg.* 294/2021 ("BC FIPPA Personal Information Disclosure for Storage Outside of Canada Regulation") Applicable in limited circumstances: *E-Health (Personal Health Information Access and Protection of Privacy) Act*, SBC 2008, c. 38 ("E-Health Act") *Pharmaceutical Services Act*, SBC 2012, c. 22	No, under BC PIPA for private "organizations". Health professionals operating in the private sector are subject to private sector privacy legislation (BC PIPA), while health professionals who operate within public health care organizations, such as hospitals, health authorities, and the health ministries, are subject to public sector privacy legislation (BC FIPPA). **BC PIPA** BC PIPA does not prohibit the transfer of personal information for outsourcing arrangements involving foreign-based service providers. However, obligations with respect to accountability, safeguarding, and notice will apply. For transborder data requirements under BC PIPA, see the chart on private sector privacy legislation below. **BC FIPPA** Disclosure outside of Canada (BC FIPPA) 33.1 A public body may disclose personal information outside of Canada only if the disclosure is in accordance with the regulations, if any, made by the minister responsible for this Act. BC FIPPA Personal Information Disclosure for Storage Outside of Canada Regulation *Additional privacy impact assessment requirements* 2(1) The head of a public body must make an assessment in accordance with subsection (2) with respect to each of the public body's programs, projects and systems in which personal information that is sensitive is disclosed to be stored outside of Canada. (2) An assessment under subsection (1) must be made in a privacy impact assessment conducted under section 69 of the Act. Section 2 does not apply (a) to a program, project or system in existence at the time this regulation is brought into force, or (b) respecting disclosures made under section 33(2)(f) of the Act [information that is required to be made public]. Reasonable security measures for personal information disclosures outside Canada (Guidance) See also the OIPC BC's guidance document: "Reasonable security measures for personal information disclosures outside Canada" (March 2022), intended to help public bodies understand their safeguarding obligations under s. 30 of FIPPA in the transborder context.

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
	E-Health Act Disclosure of personal health information (s. 5) A designation order may authorize the disclosure of personal health information only for one or more of the following purposes: (a) if disclosure is inside Canada, a purpose set out in section 4(a) to (g) [collection and use of personal health information]; (…) (c) if disclosure is inside or outside Canada, a purpose set out in section 4(h) or (i). Disclosure for health research purposes (s. 14) (1) A person may request protected information for a health research purpose only by submitting to the data stewardship committee (a) a request in the form and in the manner required by the data stewardship committee, and (b) information required by the data stewardship committee for the purposes of evaluating the request. (2) The data stewardship committee may approve the request if both of the following apply: (a) in the case of a request to disclose personal health information, all of the requirements set out in subsection (2.1) are met; (b) in the case of a request to disclose protected information outside Canada, there is express consent, in writing, to the disclosure from each person who is the subject of the protected information. Disclosure of personal information (s. 18) (2) An administrator may disclose personal health information inside or outside Canada from a health information bank for one or more of the following purposes: (a) a purpose described in section 33 (2) (a), (e), (h), (l), (m), (o), (p), (t), (u) or (v), (3) (a), (b) or (c), (8) or (9) of the Freedom of Information and Protection of Privacy Act, or (b) a purpose for which the person who is the subject of the personal health information has expressly consented in writing. ***Pharmaceutical Services Act*, SBC 2012, c. 22** Collection, use and disclosure of personal information (s. 22) (1) The minister may collect personal information under this Act for one or more of the following purposes:

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
	(a) to provide health services, or facilitate care, in relation to drugs, devices, substances and related services; (b) to administer this Act; (c) for a prescribed purpose. (…) (3) The minister may disclose, outside Canada, personal information collected under subsection (1) for one or both of the following purposes: (a) to conduct or facilitate research into health issues; (b) to assess and address threats to public health. Disclosure of personal information (s. 23) (2) The minister may disclose personal information under this Act inside or outside Canada for one or more of the following purposes: (a) for a purpose described in section 33 (2) (a), (e), (h), (l), (m), (o), (p), (t), (u) or (v), (3) (a), (b) or (c), (8) or (9) of the Freedom of Information and Protection of Privacy Act only; (b) for a purpose to which the person who is the subject of the personal information has consented in writing.
Alberta Office of the Information and Privacy Commissioner of Alberta *Health Information Act* , RSA 2000, c H-5 ("Alberta HIA") *Health Information Regulation*, Alta Reg 70/2001 ("Alberta HI Reg.")	Yes. Written agreement required (s. 60(1)(b), Alberta HIA) • A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will 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 Content of Written Agreement (s. 8(4), Alberta Reg.) • 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 o provides for the custodian to retain control over the health information, o adequately addresses the risks associated with the storage, use or disclosure of the health information,

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
	○ requires the person to implement and maintain adequate safeguards for the security and protection of the health information, ○ allows the custodian to monitor compliance with the terms and conditions of the agreement, and ○ contains remedies to address any non-compliance with or breach of the terms and conditions of the agreement by the other person. ***[Note: The requirements set out above are consistent with the requirements and regulatory expectations for service provider agreements generally.]***
Saskatchewan Office of the Saskatchewan Information and Privacy Commissioner *Health Information Protection Act*, SS 1999, c H-0.0.21 *Health Information Protection Regulations*, RRS c H-0.021 Reg 1	None.
Manitoba Manitoba Ombudsman Access and Privacy Division *Personal Health Information Act*. C.C.S.M. c. P33.5 ("Manitoba PHIA") *Personal Health Information Regulation*, Regulation 245/97	None.
Québec Commission d'accès à l'information du Québec *An Act Respecting Access To Documents Held By Public Bodies And The Protection Of Personal Information*, CQLR c A-2.1 ("Québec Public Sector Privacy Act") *Act respecting health and social services information* ("Québec Health Privacy Act")	Yes. **Québec Public Sector Privacy Act** 70.1. Before releasing personal information outside Québec or entrusting a person or a body outside Québec with the task of holding, using or releasing such information on its behalf, a public body must ensure that the information receives protection equivalent to that afforded under this Act. If the public body considers that the information referred to in the first paragraph will not receive protection equivalent to that afforded under this Act, it must refuse to release the information or refuse to entrust a person or a body outside Québec with the task of holding, using or releasing it on its behalf.

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
	159.2. Every person who knowingly contravenes section 67.2 or the second paragraph of section 70.1 is liable to a fine of $5,000 to $50,000 and, in the case of a second or subsequent conviction, to a fine of $10,000 to $100,000. Public bodies must conduct a formal privacy impact assessment (PIA) before communicating personal information outside of Québec. In particular, public bodies must take into account: (1) the sensitivity of the information, (2) the purposes for which the information is to be used, (3) the protection measures, including contractual measures, that would apply to the information, and (4) the legal framework (including personal information protection principles) applicable in the jurisdiction where the information will be transferred. A public body may only communicate the information outside Québec if the PIA establishes that the information would receive adequate protection, in particular in light of generally recognized principles regarding the protection of personal information. The release of the information must be the subject of a written agreement that takes into account, in particular, the results of the PIA and, if applicable, the terms agreed on to mitigate the risks identified in the PIA. The same applies where the public body entrusts a person or body outside Québec with the task of collecting, using, releasing or keeping such information on its behalf. These requirements do not apply when (a) the information must be communicated due to the urgency of a situation that threatens the life, health or safety of the individual to whom the personal information relates, (b) the information is released to a public body or an agency of another government if it is clearing for the benefit of the individual, or (c) the information in question is within the scope of an international commitment or agreement or related to a critical public health matter. (Québec Public Sector Privacy Act, s. 70.1). A person whose personal information is collected by another person on behalf of a public body must be informed of the following, if applicable: the name of the person collecting the information on behalf of the public body, the name of the third persons or categories of third persons to whom it is necessary to release the information for the purposes for which the information is collected, and the possibility that the information could be released outside Québec.

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
	(Québec Public Sector Privacy Act, s. 65) **Québec Health Privacy Act** This statute applies to a wide range of organizations, defined as "health and social services bodies", that collect, use and/or disclose health and social services information[3]. **PIA Requirement.** 78. Before giving a mandate or entering into a contract of enterprise or for services involving the communication of information outside Québec, the body holding the information must ensure that a privacy impact assessment has been conducted. Section 45 applies, with the necessary modifications, to such an assessment. The mandate may be given or the contract of enterprise or for services entered into only if the assessment shows that the information would receive adequate protection, in particular in light of generally recognized principles regarding the protection of personal information. The agreement referred to in section 77 must then take into account, in particular, the results of the assessment and, if applicable, the terms agreed on to mitigate the risks identified in the assessment. The same applies where a body entrusts a person or group outside Québec with the task of collecting, using, communicating or keeping such information on its behalf. 45. The privacy impact assessment referred to in subparagraph 2 of the second paragraph of section 44 must be proportionate to the sensitivity of the information concerned, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored. Moreover, where the research project involves the communication of information outside Québec, the assessment must take into account (1) the sensitivity of the information; (2) the purposes for which it is to be used;

[3] "Health and social services information" is any information that allows a person to be identified, even indirectly, and that has any of the following characteristics: (1) it concerns the person's state of physical or mental health and his or her health determinants, including the person's medical or family history; (2) it concerns any material taken from the person, including biological material, collected in the context of an assessment or treatment, or any implants, ortheses, prostheses or other aids that compensate for a disability of the person; (3) it concerns the health services or social services provided to the person, including the nature of those services, their results, the location where they were provided and the identity of the persons or groups that provided them; (4) it was obtained in the exercise of a function under the Public Health Act (chapter S-2.2); or (5) any other characteristic determined by government regulation.

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
	(3) the protection measures, including those that are contractual, that would apply to it; and (4) the legal framework applicable in the State in which the information would be communicated, including the rules for the protection of health and social services information applicable in that State. **Written Agreement Requirement**. 77. A body may communicate information it holds to a person or group to whom or which it entrusts the carrying out of a mandate or with whom or which it enters into a contract of enterprise or for services, other than a contract for the provision of health services or social services, if the information is necessary for carrying out the mandate or performing the contract. Such a mandate or contract must be, as applicable, given or entered into in writing and, where it is given to or entered into with a person or group that is not a body, it must, on pain of nullity, set out (1) the provisions of this Act that apply to the information communicated to the mandatary or the person performing the contract; (2) the measures to be taken by the person or group to ensure, at all times throughout the carrying out of the mandate or performance of the contract, (a) that the confidentiality of the information is respected; (b) that the information is protected, which measures must comply with the information governance rules referred to in section 90 and the special rules defined by the network information officer under section 97; and (c) that the information is used only for carrying out the mandate or performing the contract; and (3) the following obligations to be complied with by the person or group that carries out the mandate or performs the contract: (a) send to the body, before any communication, a confidentiality agreement completed by every person to whom the information may be communicated or who may use it in carrying out the mandate or performing the contract; (b) use only technological products or services authorized by the body to collect, keep, use or communicate the information where the mandate is carried out or the contract is performed remotely; (c) immediately notify the person in charge of the protection of information within the body of any violation or attempted violation by any person of any of the obligations relating to the protection of information that are provided for by the agreement; (d) allow the body to conduct any verification or investigation relating to the protection of the information; (e) send to the body, free of charge and whenever it so requires, all information obtained or produced in carrying out the mandate or performing the contract; and

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
	(f) not keep the information at the end of the mandate or contract, and destroy it in a secure manner. A person or group that retains a third person to carry out a mandate or perform a contract of enterprise or for services must notify the body concerned. The third person is subject to the same obligations as those imposed on the person or group in accordance with the second paragraph. However, the third person must send the person or group the confidentiality agreement required under subparagraph a of subparagraph 3 of the second paragraph and the notice required under subparagraph c of that subparagraph.
New Brunswick Office of the Integrity Commissioner for New Brunswick *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05 ("NB PHIPAA") *General Regulation*, NB Reg 2010-112 ("NB Reg.")	No, assuming that where a transfer is made by a public body, the transfer is for information management or technology services only. While there are restrictions on a public body's storage and access to PHI outside of Canada (see s. 55(2)(c) of the NB PHIPAA below), there is an exception under s. 22 of the NB Reg permitting information managers providing a public body with information management or technology services to store health information in their custody or control outside Canada. **NB PHIPAA** Express Consent (s. 19, NB PHIPAA) 19(1) Unless otherwise provided in this Act, express consent of an individual is required in relation to the collection, use or disclosure of his or her personal health information by a custodian, including when the custodian discloses information to (…) (d) a person outside New Brunswick Requirements for retention, storage and secure destruction of information (s. 55(2), NB PHIPAA) 55(2) Unless otherwise provided in the regulations, a public body shall ensure that personal health information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies: (a) if the individual to whom the information relates has identified the information and has consented, in the manner prescribed by regulation, to it being stored in another jurisdiction; (b) if the information is stored in another jurisdiction for the purpose of disclosure allowed under this Act; (c) if the information was disclosed for the purposes of (i) a payment to be made to or by the Province or a public body, (ii) authorizing, administering, processing, verifying or cancelling a payment to be made to or by the Province or a public body, or (iii) resolving an issue regarding a payment to be made to or by the Province of or a public body.

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
Nova Scotia The Office of the Information & Privacy Commissioner *Personal Health Information Act*, SNS 2010, c 41 ("Nova Scotia PHIA") *Personal Health Information Regulations*, NS Reg 217/2012 *Personal Information International Disclosure Protection Act*, SNS 2006, c 3 *("*PIIDP Nova Scotia*")*	Health custodians operating in both the public and private sectors are subject to Nova Scotia PHIA, which allows transborder sharing of personal health information with an agent for processing[4]; however, transborder outsourcing restrictions under PIIDP Nova Scotia will apply to health custodians that are *public bodies*. **PIIDP Nova Scotia** To the extent that public sector health custodians are also public bodies under the PIIDP Nova Scotia (which are defined to include hospitals), they must ensure that personal information in their custody or control, *and that of their service providers*, is stored and accessed only in Canada unless the individuals have consented, in prescribed form, to processing outside Canada or subject to other exceptions. Information to be stored and accessed in Canada (s. 5(1), PIIDP Nova Scotia) A public body shall ensure that personal information in its custody or under its control and a service provider or associate of a service provider shall ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless a) where the individual the information is about has identified the information and has consented, in the manner prescribed by the regulations, to it being stored in or accessed from, as the case may be, outside Canada; b) where it is stored in or accessed from outside Canada for the purpose of disclosure allowed under this Act; or c) the head of the public body has allowed storage or access outside Canada pursuant to subsection (2). (2) The head of a public body may allow storage or access outside Canada of personal information in its custody or under its control, subject to any restrictions or conditions the head considers advisable, if the head considers the storage or access is to meet the necessary requirements of the public body's operation.

[4] Although Nova Scotia PHIA contains provisions relating to disclosures outside Nova Scotia (s. 44), "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." (s. 29).

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
	(3) Where the head of a public body makes a decision pursuant to subsection (2) in any year allowing storage or access outside Canada, the head shall, within ninety days after the end of that year, report to the Minister all such decisions made during that year, together with the reasons therefor. (4) In providing storage, access or disclosure of personal information outside Canada, a service provider shall only collect and use such personal information that is necessary to fulfill its obligation as a service provider, and shall at all times make reasonable security arrangements to protect any personal information that it collects or uses by or on behalf of a public body. Disclosure outside Canada (s. 9(1), PIIDP Nova Scotia) 9 (1) A public body shall ensure that personal information in its custody or under its control and a service provider or associate of a service provider shall ensure that personal information in its custody or under its control is disclosed outside Canada only as permitted pursuant to this Section. (2) A public body, service provider or associate of a service provider may disclose outside Canada personal information in its custody or under its control […] (b) where the individual the information is about has identified the information and consented, in writing, to its disclosure inside or outside Canada, as the case may be
Prince Edward Island Office of the Information and Privacy Commissioner *Health Information Act*, R.S.P.E.I. 1988, c. H-1.41 ("PEI HIA") *Health Information Regulations*, PEI Reg EC359/17 ("PEI HIA Regs")	None.[5]

[5] Under the PEI HIA, "[a] custodian may disclose personal health information relating to an individual that is collected in the province to a person outside the province without the consent of the individual only in the circumstances described in subsections 23(7), (10) and (13) or as specified in the regulations." (s. 35; see also s. 5.1 of the PEI HIA Regs).

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 the PEI HIA. (s. 23(13)(f), PEI HIA).

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
Newfoundland & Labrador Office of the Information and Privacy Commissioner Newfoundland and Labrador *Personal Health Information Act,* SNL 2008 Chapter P-7.01 ("Newfoundland PHIA") *Personal Health Information Regulations,* Regulation 38/11	Yes.[6] Safeguards required (s. 13, Newfoundland PHIA) (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. (3) The information policies and procedures referred to above shall include policies and procedures to 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 ***[Note: The requirements set out above are consistent with the requirements and regulatory expectations for service provider agreements generally.]***
Yukon Information and Privacy Commissioner *Health Information Privacy and Management Act,* S.Y. 2013, c.16 ("Yukon HIPMA") *Health Information General Regulation*, YOIC 2016/159 ("Yukon HI Reg.")	None.[7]
Northwest Territories Office of the Information and Privacy Commissioner	Yes. Safeguards Required (s. 85(1)(b), NTW HIA)

[6] Under PHIA Newfoundland, "[a] custodian may disclose personal health information about an individual collected in the province to a person outside the province but only where the disclosure is permitted by this Act or the regulations" (s. 47(1)(b)). Section 39(1)(f) further provides that "[a] custodian may disclose personal health information without the consent of the individual who is the subject of the information to an information manager in accordance with section 22".

[7] Although the Yukon HIPMA contains notice requirements relating to disclosures outside Yukon (s. 41(1)(d)), "the transmission of the personal health information between a custodian and an agent of that custodian" is considered a "use" (s. 2(1)).

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
Health Information Act S.N.W.T. 2014, c.2 ("NWT HIA") *Health Information Regulations*, N.W.T. R-089-2015 ("NWT HIA Regs")	• A health information custodian shall take reasonable measures to maintain administrative, technical and physical safeguards for the protection of personal health information, including for protection 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. Specific Safeguards (s. 13, NWT HIA Reg.) • The administrative, technical and physical safeguards required under section 85 of the Act must include o measures to protect personal health information through an assessment of re-identification risk and the application of de-identification procedures as required; o measures to protect network infrastructure from interruption and unauthorized access and use; o the use of authentication and encryption to protect information stored electronically; o measures to prevent and respond to problems involving hardware and software that might threaten the security, confidentiality or integrity of personal health information; o measures to protect hardware and software from unauthorized access and use; o measures to protect personal health information stored and transported on removable media; o a requirement that personal health information be maintained in a designated area subject to appropriate security safeguards; o 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; o procedures that provide for the recording, reporting and investigation of security and privacy breaches; and o procedures that provide for effective prevention of, response to and remediation of security and privacy breaches. • 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. • A health information custodian shall review its compliance with and the effectiveness of its administrative, technical and physical safeguards on an annual basis ***[Note: The requirements set out above are consistent with the requirements and regulatory expectations for service provider agreements generally.]***
Nunavut	None.

Province, Regulator & Health Privacy Legislation	Statutory Provisions on Transborder Service Provider Arrangements
Office of the Information and Privacy Commissioner of Nunavut *Public Health Act,* S.Nu.2016, c.13 *Public Health Administrative Regulations, R-047-2019*	

KEY TRANSBORDER STATUTORY REQUIREMENTS UNDER PRIVATE SECTOR PRIVACY LEGISLATION		
Jurisdiction, Regulator & Private Sector Privacy Legislation	**Statutory Provisions on Transborder Service Provider Arrangements**	**Regulatory Guidance**
Federal Office of the Privacy Commissioner of Canada ("OPC") *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("PIPEDA")	• Canadian private sector privacy statutes do not prohibit the transfer of personal information for outsourcing arrangements involving foreign-based service providers (including affiliates). However, obligations with respect to accountability, safeguarding, and notice will apply. • As part of meeting their accountability and safeguarding obligations, organizations must take into consideration all of the elements surrounding the transfer, including by assessing the foreign regime (such as the geopolitical environment, national security laws and privacy regime) and the sensitivity of the personal information it intends to transfer. Organizations must take steps (including by contractual or other means) to provide a comparable level of protection while personal information is being processed by the third party to whom it is transferred. • Organizations are required to provide notice to individuals as part of their general openness obligations and be transparent regarding the use of foreign service providers and potential access by/disclosure of data to courts, law enforcement and governmental authorities pursuant to the laws of the foreign jurisdiction. **Resources:** PIPEDA, Principles 4.1 (see, in particular, 4.1.3), 4.7 and 4.8; OPC Guidelines for Processing Personal Data Across Borders (2009).	Guidelines for Processing Personal Data Across Borders OPC Key Findings: • PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. • PIPEDA does establish rules governing transfers for processing. • A transfer for processing is a "use" of the information; it is not a disclosure. Assuming the information is being used for the purpose it was originally collected, additional consent for the transfer is not required. • The transferring organization is accountable for the information in the hands of the organization to which it has been transferred. • Organizations must protect the personal information in the hands of processors. The primary means by which this is accomplished is through contract. • No contract can override the criminal, national security or any other laws of the country to which the information has been transferred. • It is important for organizations to assess the risks that could jeopardize the integrity, security and confidentiality of customer personal information when it is transferred to third-party service providers operating outside of Canada. • Organizations must be transparent about their personal information handling practices. This includes advising customers that their personal information may be sent to another jurisdiction for processing and that while the information is in another jurisdiction it may be accessed by the courts, law enforcement and national security authorities.

KEY TRANSBORDER STATUTORY REQUIREMENTS UNDER PRIVATE SECTOR PRIVACY LEGISLATION		
Jurisdiction, Regulator & Private Sector Privacy Legislation	**Statutory Provisions on Transborder Service Provider Arrangements**	**Regulatory Guidance**
British Columbia Office of the Information and Privacy Commissioner of British Columbia *Personal Information Protection Act*, S.B.C. 2003, c. 63 ("BC PIPA")	• Same as Federal above.	
Alberta Office of the Information and Privacy Commissioner of Alberta *Personal Information Protection Act*, S.A. 2003, c. P-6.5 ("Alberta PIPA")	**Notice Obligations** • Organizations subject to Alberta PIPA may transfer data to processors outside Canada without consent, *provided* specific notification requirements are met. • The notice regarding the use of foreign service providers must be provided (in writing or orally) before or at the time of collection or transfer of the personal information and must specify: 1. The way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada; and 2. The name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization. **Policies and Procedures** • In addition, Alberta organizations that use foreign service providers must include the following information in their policies and procedures (available upon request):	

KEY TRANSBORDER STATUTORY REQUIREMENTS UNDER PRIVATE SECTOR PRIVACY LEGISLATION		
Jurisdiction, Regulator & Private Sector Privacy Legislation	**Statutory Provisions on Transborder Service Provider Arrangements**	**Regulatory Guidance**
	1. The countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur; and 2. The purposes for which the third party service provider outside Canada has been authorized to collect, use or disclose personal information for or on behalf of the organization. **Resources**: PIPA AB, s. 6(2) and 13.1(2) and (3)	
Québec Commission d'accès à l'information du Québec ("CAI") *An Act respecting the protection of personal information in the private sector*, CQLR c. P-39.1 ("Québec Privacy Act")	The Québec Privacy Act requires an organization to take "reasonable steps" to ensure that personal information transferred to service providers outside Québec will not be used for other purposes and will not be communicated to third parties without consent (except under certain exceptions prescribed in the Act). Organizations must conduct a formal privacy impact assessment (PIA) before communicating personal information outside of Québec. In particular, organizations must take into account: (1) the sensitivity of the information, (2) the purposes for which the information is to be used (3) the protection measures, including contractual measures, that would apply to the information, and (4) the legal framework (including personal information protection principles) applicable in the jurisdiction where the information will be transferred. An organization may only communicate the information outside Québec if the PIA establishes that the information would receive adequate protection in light of generally recognized principles regarding the protection of personal information. The communication of the information must be the subject of a written agreement that takes into account, in particular, the results of the PIA	Guide d'accompagnement: Réaliser une évaluation des facteurs relatifs à la vie privée

KEY TRANSBORDER STATUTORY REQUIREMENTS UNDER PRIVATE SECTOR PRIVACY LEGISLATION		
Jurisdiction, Regulator & Private Sector Privacy Legislation	**Statutory Provisions on Transborder Service Provider Arrangements**	**Regulatory Guidance**
	and, if applicable, the terms agreed on to mitigate the risks identified in the PIA. The same applies where the organization entrusts a person or body outside Québec with the task of collecting, using, communicating or keeping such information on its behalf. However, these requirements do not apply when the information must be communicated due to the urgency of a situation that threatens the life, health or safety of the individual to whom the personal information relates. **Resources:** Québec Privacy Act, s.17. A person whose information is collected must be informed of the following, if applicable: • the name of the third person for whom the information is being collected, • the name of the third persons or categories of third persons to whom it is necessary to communicate the information for the purposes for which the information is collected, and • the possibility that the information could be communicated outside Québec. **Resources:** Québec Privacy Act, s. 8. An organization that communicates personal information in violation of the law may be subject to: • a monetary penalty of up $10,000,000 or, if greater, the amount corresponding to 2% of worldwide turnover for the preceding fiscal year; or	

KEY TRANSBORDER STATUTORY REQUIREMENTS UNDER PRIVATE SECTOR PRIVACY LEGISLATION		
Jurisdiction, Regulator & Private Sector Privacy Legislation	**Statutory Provisions on Transborder Service Provider Arrangements**	**Regulatory Guidance**
	• a fine of up to $25,000,000, or, if greater, the amount corresponding to 4% of worldwide turnover for the preceding fiscal year. **Resources:** Québec Privacy Act, ss. 90.1, 90.12, 91.	