ACCESSPRIVACY BY OSLER

Canadian Personal Health Information: Comparative Table of Breach Notification Regimes[1]

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
Ontario *Personal Health Information and Protection of Privacy Act, 2004* ("PHIPA") Note: In this province, there is a specific personal data breach notification requirement in the health sectors, set out in the PHIPA. Note: "HIC" means Health Information Custodian. A HIC is a listed individual or organization under PHIPA that, as a result of his or its power or duties, has custody or control of personal health information. Examples of HICs include health care practitioners, hospitals, pharmacies, and	**Information and Privacy Commissioner of Ontario** 2 Bloor Street East, Suite 1400 Toronto, Ontario M4W 1A8 Phone (Toronto Area): 416-326-3333 Toll Free: 1-800-387-0073 Fax: 416-325-9188 reportabreach@ipc.on.ca	Notice to the Information and Privacy Commissioner of Ontario ("IPC" or "Commissioner") is required where the theft, loss or unauthorized use or disclosure meet prescribed requirements. (PHIPA, s. 12(3)). Amendments to O. Reg. 329/04, which came into force on October 1, 2017, prescribe that the HIC must notify the Commissioner under PHIPA, s. 12(3) in any of the following circumstances: • The HIC has reasonable grounds to believe that personal health information in its custody or control was used or disclosed without authority by a person who knew or ought to have known that they were using or disclosing the information without authority. • The HIC has reasonable grounds to believe that personal health information in its custody or control was stolen. • The HIC has reasonable grounds to believe that, after an initial loss or unauthorized use or disclosure of personal health information in its custody or control, the personal health information was or will be further used or disclosed without authority. • The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures	There is no time limit set out in law or regulation, but the IPC's guidance recommends that HICs do so "as soon as reasonably practical".	HICs may report a privacy breach to the IPC by mail, fax, or by completing the Report a Privacy Breach at your Organization page.	HICs may report a privacy breach to the IPC by mail, fax, or by completing the Report a Privacy Breach at your Organization page. IPC's Breach Report Form requests the following information: • Description of the circumstances surrounding the privacy breach • Nature of personal health information that was lost or stolen, or used or disclosed without authority • Steps taken to contain the breach • Whether, when and how individuals were notified • Steps taken to investigate and remediate the breach • Steps taken to prevent future privacy breaches and steps that remain to be taken

[1] Note: Several provincial health data breach reporting and notification frameworks also contain record keeping requirements. These records are typically required so that an organization can demonstrate why it determined it was not required to notify individuals of the data breach. For more information regarding such record-keeping requirements, please see our Health Information Retention hub.

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification

laboratories (PHIPA, s.3(1)).		of personal health information in the custody or control of the HIC.
		• The HIC is required to give notice to a College of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.
		• The HIC would be required to give notice to a College, if an agent of the HIC were a member of the College, of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information.
		• The HIC determines that the loss or unauthorized use or disclosure of personal health information is significant after considering all relevant circumstances, including the following:
		  • Whether the personal health information that was lost or used or disclosed without authority is sensitive.
		  • Whether the loss or unauthorized use or disclosure involved a large volume of personal health information.
		  • Whether the loss or unauthorized use or disclosure involved many individuals' personal health information.
		  • Whether more than one HIC or agent was responsible for the loss or unauthorized use or disclosure of the personal health information. (O. Reg. 329/04, s. 6.3(1)).
		The IPC has recently released guidance summarizing the HIC's responsibilities for notifying the			

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
		Commissioner of breaches involving personal health information. Please also note that O. Reg. 329/04 requires HICs to provide the Commissioner with an annual statistical breach report. (O. Reg. 329/04, s. 6.4(1)) on or before March 1 in each year starting in 2019. The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner (O. Reg. 329/04, s. 6.4(2)) and shall set out the number of times in the previous calendar year that each of the following occurred: 1. Personal health information in the HIC's custody or control was stolen. 2. Personal health information in the HIC's custody or control was lost. 3. Personal health information in the HIC's custody or control was used without authority. 4. Personal health information in the HIC's custody or control was disclosed without authority. (O. Reg. 329/04, s. 6.4(1)).			
	Individuals	A HIC that has custody or control of personal health information about an individual must notify the individual at the first reasonable opportunity if the information is stolen, lost or used or disclosed without authority (the definition of "use" includes to view, handle or otherwise deal with the information) (PHIPA, s. 12(2)).	Notification must be provided "at the first reasonable opportunity" (PHIPA, s. 12(2)).	Notification can be by telephone or in writing. There are many factors to consider when deciding on the best form of notification (e.g., the sensitivity of the PHI). If unsure, contact the IPC to discuss the most appropriate form of notification.	PHIPA requires that the notice to individuals include a statement that the individual is entitled to make a complaint to the IPC (PHIPA, s. 12(2)(b)). In addition, guidance from the ON IPC indicates that, when notifying individuals affected by the breach, HICs should: • provide details of the breach, including the extent of the breach and what personal health information was involved; other ON IPC guidance advises that the following details of the breach be included in the notification:

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
					○ the date of the breach; ○ a description of the nature and scope of the breach; ○ a description of the personal health information that was subject to the breach; and ○ the measures implemented to contain the breach. • advise of the steps they are taking to address the breach, and that individuals are entitled to make a complaint to the IPC. (HICs should advise individuals if they have reported the breach to the ON IPC.) • provide contact information for someone within their organization who can provide additional information and assistance, and answer questions.
Québec *Act respecting health and social services information* ("QC Heath Act") *Regulation respecting the application of certain provisions of the Act respecting health and social services information* (the "Regulation")	**Commission d'accès à l'information** 525, René-Lévesque Est, Office 2.36 Québec (Québec) G1R 5S0 Phone : 418 528-7741; or toll free: 1 888 528-7741 Fax : 418 529-3102	Notice to the Commission d'accès à l'information ("CAI") and the Ministère de la Santé et des Services Sociaux (the "Minister") is required where a confidentiality incident presents a "risk of serious injury". The body must also notify any person whose information is impacted by the incident, and may also notify any person or group that could reduce the risk. A "confidentiality incident" means access to information or any other use or communication of information not authorized by law, the loss of information or any other breach of its protection (QC Health Act, s. 108). In assessing the risk of injury, a health and social services body must consult the person in charge of the protection of information within the body and consider the following factors: • the sensitivity of the information concerned, • the anticipated consequences of its use, and	Notification must be provided "promptly" (QC Health Act, s. 108).	Notice to the CAI and the Minister must be provided in writing (Regulation, s. 11). The CAI has made available a Confidentiality Incident Report Form (only available in French) to assist bodies in reporting a confidentiality incident at the following email address: cai.communications@cai.gouv.qc.ca. According to the Minister's Reference Guide on the QC Health Act, bodies may notify the Minister of a confidentiality incident using the following email address: MSSS_incident_PRP@msss.	The Regulation requires that the notice to the CAI and Minister include: • name of the body affected by the incident; • name and contact information of the person to be contacted in that body with regard to the incident; • description of the information concerned by the incident or, if that information is not known, the reasons why it is impossible to provide such a description; • description of the circumstances of the incident and what caused it, if known; • date or time period when the body became aware of the incident; • number of persons concerned by the incident and the number of those who reside in Québec or, if that is not known, the approximate numbers; • description of the elements that led that body to conclude that there is a risk of serious injury to the persons concerned, such as the sensitivity of the information

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
	cai.communications@cai.gouv.qc.ca **Ministère de la Santé et des Services sociaux** Centre de commerce mondial de Montréal 393, rue Saint-Jacques 4e étage, suite 400 Montréal (Québec) H2Y 1N9 Phone : 514 873-3700 MSSS_incident_PRP@msss.gouv.qc.ca	• the likelihood that such information will be used for injurious purposes (QC Health Act, s. 109).		gouv.qc.ca.	concerned, any possible ill-intentioned uses of such information, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes; • measures the body has taken or intends to take to notify the persons concerned by the incident and the date on which such persons were notified, or the expected time for the notification; • measures the body has taken or intends to take after the incident occurred, including those aimed at reducing the risk of injury or mitigating any such injury and those aimed at preventing new incidents of the same nature, and the date or time period on which the measures were taken or the expected time limit for taking the measures; and • if applicable, an indication that a person or body outside Québec that exercises similar functions to those of the CAI with respect to overseeing the protection of personal information has been notified of the incident (Regulation, s. 11)

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
	Individuals	Notice to individuals is required when the confidentiality incident presents a risk of serious injury (QC Health Act, s. 108). In assessing the risk of injury, a body must consult the person in charge of the protection of information within the body and consider the following factors: • the sensitivity of the information concerned, • the anticipated consequences of its use, and • the likelihood that such information will be used for injurious purposes (QC Health Act, s. 109).	There is no time limit set out in law.	The statute requires notice to be provided to the impacted individuals directly, although there are limited instances in which indirect notification is permitted (Regulation, s. 14).	The Regulation requires that the notice to impacted individuals include: • description of the information concerned by the incident or, if that information is not known, the reason why it is impossible to provide such a description; • brief description of the circumstances of the incident; • date or time period when the incident occurred or, if that is not known, the approximate time period; • brief description of the measures the body has taken or intends to take after the incident occurred in order to reduce the risks of injury; • measures that the body suggests the person concerned take in order to reduce the risk of injury or mitigate any such injury; and • contact information where the person concerned may find out more about the incident. (Regulation, s. 13).

British Columbia
 	
Personal Information Protection Act ("PIPA").
 	
Note: This province has its own personal data breach notification rule, under the PIPA.
	Information and Privacy Commissioner of British Columbia
	
	PO Box 9038 Stn. Prov. Govt. Victoria B.C. V8W 9A4
	
	Phone: (250) 387-5629
	
	info@oipc.bc.ca
		There is no general requirement under the PIPA to notify the Office of the Information and Privacy Commissioner for British Columbia ("**OIPC**") or affected individuals in the event of a breach. However, the OIPC has published guidance indicating that notification to affected individuals, the OIPC, and other third-parties (such as police, insurers, and regulatory bodies) should be provided in some cases.
		
		OIPC guidance provides the following factors to assist in determining whether or not to notify the OIPC:
		
		• The sensitivity of the personal information;
		• Whether the disclosed information could be used to commit identity theft;
			A deadline for notification to the OIPC has not been specified in guidance. It is generally expected that notification occur as soon as possible following the breach.	N/A	To notify the OIPC, the OIPC has created a Privacy Breach Checklist (page 11) which requests the following information:
					
					• Contact information for the organization reporting the breach;
					• A description of the incident including:
					  ○ The nature of the breach and its cause;
					  ○ Date of incident;
					  ○ Date incident discovered;
					  ○ Location of incident;
					  ○ Estimated number of individuals affected; and
					  ○ Type of individuals affected (e.g. client/customer/patient, employee);

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
		• Whether there is a reasonable chance of harm from the disclosure, including non-pecuniary losses; • The number of people affected by the breach; • Whether the information was fully recovered without further disclosure; • Whether the organization requires assistance in developing a procedure for responding to the privacy breach, including notification; and/or • To ensure steps taken comply with the organization's obligations under privacy legislation.			• A description of the personal information involved; • The physical, technical and organizational security measures; • Identification of the type of harms that may result from the breach; • Who has been notified (e.g. privacy officer, policy, affected individuals); • Information included in notification to individuals and a copy of the notification letter; • Description of immediate steps taken to contain and reduce the harm of the breach; and • Long term-strategies to correct the situation.
	Individuals	OIPC guidance indicates that individuals should be notified in order to avoid or mitigate harm to the individual whose personal information has been inappropriately collected, used or disclosed. The OIPC has provided the following factors to assist in determining whether or not to notify affected individuals: • Contractual obligations that require notification; • There is a risk of identity theft or fraud (usually because of the type of information lost/stolen/accessed/disclosed, such as SIN, banking information, identification numbers); • There is a risk of physical harm (if the loss puts an individual at risk of stalking or harassment); • There is a risk of hurt, humiliation or damage to reputation (for example when the information lost includes medical or disciplinary records);	OIPC guidance indicates that notification should occur as soon as possible following the breach (unless law enforcement has indicated that notification would impede a criminal investigation) .	Direct notification is preferred – by phone, by letter, or in person. Indirect notification – via websites, posted notices, or media reports – should generally only occur where direct notification could cause further harm, is cost-prohibitive, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.	OIPC guidance indicates that notification should be provided directly (unless direct notification could cause further harm, is cost prohibitive or contact information is lacking) and should include the following pieces of information: • Date of the breach; • Description of the breach; • Description of the information inappropriately accessed, collected, used or disclosed; • Risk(s) to the individual caused by the breach; • The steps taken so far to control or reduce the harm; • Future steps planned to prevent further privacy breaches; • Steps the individual can take to further mitigate the risk of harm (e.g. how to contact credit reporting agencies to set up a credit watch, information explaining how to change a personal health number or driver's licence number);

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
		• There is a risk of loss of business or employment opportunities (if the loss of information could result in damage to the reputation of an individual, affecting business or employment opportunities); or • There is a risk of loss of confidence in the organization and/or good customer/client relations dictates that notification is appropriate.			• Contact information of an individual within the organization who can answer questions or provide further information; and • Privacy Commissioner contact information and the fact that individuals have a right to complain to the Office of the Information and Privacy Commissioner. If the organization has already contacted the Privacy Commissioner, this detail should be included in the notification letter.
Alberta *Health Information Act* ("HIA") Note: "OIPC" or "Commissioner" means the Office of the Information and Privacy Commissioner of Alberta.	**Information and Privacy Commissioner of Alberta** Suite 2460, 801 6 Avenue SW Calgary, AB T2P 3W2 Phone: 403-297-2728 Toll-Free: 1-888-878-4044 generalinfo@oipc.ab.ca	To Custodian 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. (HIA, s. 60.1(1)) To OIPC, Minister, Affected Individuals A Custodian must as soon as practicable give notice 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 if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure. (HIA, s. 60.1(2) and (3)) A custodian must consider all relevant factors, including the factors prescribed by the regulations, in assessing for the purposes of subsection (2) whether there is a risk of harm to an individual (HIA, s. 60.1(4)).	Notice must be provided "as soon as practicable" (HIA, s. 60.1(1) and (2)). OIPC guidance advises that a breach be reported to the Commissioner as soon as possible even if all the information requested on the Privacy Breach Report Form is not yet available (e.g. the	The OIPC has made available a Privacy Breach Report Form to assist custodians in reporting a privacy breach to the Commissioner.	To Custodian A notice to a custodian under section 60.1(1) of the Act must: (a) if the custodian has established requirements respecting the notice, meet any requirements respecting form and contents established by the custodian, or (b) if the custodian has not established requirements respecting the notice, be in writing and include (i) a description of the circumstances of the loss or unauthorized access or disclosure, (ii) the date on which or period of time within which the loss or unauthorized access or disclosure occurred, (iii) the date on which the loss or unauthorized access or disclosure was discovered, and (iv) a description of the information that was lost or that was the subject of the unauthorized access or disclosure (Health Information Regulation, s.8.2(1)). To OIPC A notice to the Commissioner must be in writing in a form approved by the Commissioner and must include:

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
		There are additional provisions that apply if a custodian considers that giving notice could reasonably be expected to result in a risk of harm to the individual's mental or physical health. (HIA, s. 60.1(5)) Assessment of risk of harm In assessing whether there is a risk of harm to an individual as a result of a loss of or an unauthorized access to or disclosure of individually identifying health information, a custodian must consider each of the following factors in addition to any other relevant factors: (a) whether there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person; (b) whether there is a reasonable basis to believe that the information has been misused or will be misused; (c) whether there is a reasonable basis to believe that the information could be used for the purpose of identity theft or to commit fraud; (d) whether there is a reasonable basis to believe that the information is of a type that could cause embarrassment or physical, mental or financial harm to or damage the reputation of the individual who is the subject of the information; (e) whether there is a reasonable basis to believe that the loss of or unauthorized access to or disclosure of the information has adversely affected or will adversely affect the provision of a health service to the individual who is the subject of the information;	organization has not completed its internal investigation or established long term strategies to correct the situation) and that additional information can be provided to the Commissioner as it becomes known.		(a) the name of the custodian who had custody or control of the information at the time of the loss or unauthorized access or disclosure, (b) a description of the circumstances of the loss or unauthorized access or disclosure, (c) the date on which or period of time within which the loss or unauthorized access or disclosure occurred, (d) the date on which the loss or unauthorized access or disclosure was discovered, (e) a non-identifying description of the type of information that was lost or that was the subject of the unauthorized access or disclosure, (f) a non-identifying description of the risk of harm to an individual as a result of the loss or unauthorized access or disclosure, including a description of the type of harm and an explanation of how the risk of harm was assessed that includes a non-identifying description of the custodian's consideration of the factors referred to in section 8.1(1), including any relevant factors not detailed in that section, (g) the number, or if the number cannot be determined, an estimate of the number, of individuals to whom there is a risk of harm as a result of the loss or unauthorized access or disclosure, (h) a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the risk of harm to an individual as a result of the loss or unauthorized access or disclosure, (i) a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the risk of a future loss or unauthorized access or disclosure, (j) a non-identifying copy of the information that has been or will be provided in the notice to the individual who is the subject of the individually identifying health information referred to in subsection (4), if applicable, together with a statement indicating the method referred to in section 103 of the Act that has been or will be used to give notice to the individual, if applicable,

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
		(f) in the case of electronic information, whether the custodian is able to demonstrate that the information was encrypted or otherwise secured in a manner that would: (i) prevent the information from being accessed by a person who is not authorized to access the information, or (ii) render the information unintelligible by a person who is not authorized to access the information; (g) in the case of a loss of information, whether the custodian is able to demonstrate that the information was lost in circumstances in which the information was: (i) destroyed, or (ii) rendered inaccessible or unintelligible; (h) in the case of a loss of information that is subsequently recovered by the custodian, whether the custodian can demonstrate that the information was not accessed before it was recovered; (i) in the case of an unauthorized access to or disclosure of information, whether the custodian is able to demonstrate that the only person who accessed the information or to whom the information was disclosed: (i) is a custodian or an affiliate, (ii) is subject to confidentiality policies and procedures that meet the requirements of section 60 of the Act, (iii) accessed the information in a manner that is in accordance with the person's duties as a custodian or affiliate and not for an improper purpose, and			(k) if the custodian is requesting the authorization of the Commissioner to give notice to an individual by substitutional service under section 103(c) of the Act, the request together with a statement of the reasons for the request, (l) the name and contact information for a person who is able to answer questions on behalf of the custodian about the loss or unauthorized access or disclosure, and (m) any other information that the custodian considers relevant (Health Information Regulation, s. 8.2(2)). The OIPC has made available a Privacy Breach Report Form to assist custodians in reporting a privacy breach to the Commissioner. A notice to the Commissioner under section 60.1(5) of the Act of a decision not to give notice to an individual must: (a) be in writing in a form approved by the Commissioner, (b) have attached as an appendix the notice required to be provided to the Commissioner in respect of the matter under section 60.1(2) of the Act, and (c) set out the total number, or if the number cannot be determined, an estimate of the total number, of individuals that the custodian expects not to give notice to on the basis set out in section 60.1(5) of the Act. (Health Information Regulation, s. 8.3). To the Minister A notice to the Minister must be in writing in a form approved by the Minister and must include the information set out in (a), (b), (e), (f), (g), (h), (l) and (m) above (Health Information Regulation, s. 8.2(3)).

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
		(iv) did not use or disclose the information except in determining that the information was accessed by or disclosed to the person in error and in taking any steps reasonably necessary to address the unauthorized access or disclosure (Health Information Regulation, s. 8.1(1)). If a custodian is able to demonstrate that a circumstance set out in (f) to (i) above applies in the case of a loss of or unauthorized access to or disclosure of individually identifying health information, the custodian is **not** required to give notice of the loss or unauthorized access or disclosure under section 60.1(2) of the Act (Health Information Regulation, s. 8.1(2))			
	Individuals	See above.	Notice to individuals must be provided directly (unless the OIPC determines that direct notification would be unreasonable in the circumstances) and within the time period prescribed by the OIPC	Notice to individuals must be provided directly (unless the OIPC determines that direct notification would be unreasonable in the circumstances).	A notice to an individual must be in writing and must include: (a) a description of the circumstances of the loss or unauthorized access or disclosure, (b) the date on which or period of time within which the loss or unauthorized access or disclosure occurred, (c) the name of the custodian who had custody or control of the health information at the time of the loss or unauthorized access or disclosure, (d) a non-identifying description of the type of information that was lost or that was the subject of the unauthorized access or disclosure, (e) a description of the risk of harm to the individual as a result of the loss or unauthorized access or disclosure, including a description of the type of harm and an explanation of how the risk of harm was assessed, (f) a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
			(PIPA, s. 37.1(1) and PIPA Regulation, s.19.1).		risk of harm to the individual as a result of the loss or unauthorized access or disclosure, (g) a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the risk of a future loss or unauthorized access or disclosure, (h) description of any steps that the custodian believes the individual may be able to take to reduce the risk of harm to the individual, (i) a statement that the individual may ask the Commissioner to investigate the loss or unauthorized access or disclosure that includes contact information for the Office of the Information and Privacy Commissioner, (j) the name and contact information for a person who is able to answer questions on behalf of the custodian about the loss or unauthorized access or disclosure, and (k) any other information that the custodian considers relevant (Health Information Regulation, s. 8.2(4)).
Saskatchewan *Health Information Protection Act* ("HIPA")	**Saskatchewan Information and Privacy Commissioner** 503 – 1801 Hamilton Street Regina SK S4P 4B4 Phone: 306-787-8350 Toll Free (within Saskatchewan): 1-877-748-2298 Fax: 306-798-1603	Guidance from Saskatchewan's Office of the Information and Privacy Commissioner ("OIPC") encourages organizations to proactively report actual or potential privacy breaches to this office. Proactive reporting to the OIPC allows this office to provide advice or guidance in responding to the incident. In this guidance, the OIPC ties privacy breaches to collections, uses or disclosures of personal health information that are contrary to HIPA, or where the personal health information is inaccurate.	While there is no prescribed timeline for notification under Saskatchewan's *Health Information Protection Act*, Guidance states that proactive reporting of privacy breaches to the IPC means that "when a trustee learns of a breach, it	N/A	While there is no prescribed content for notification, Guidance notes that an investigation report should include the following: • a summary of the incident and immediate steps taken to contain the breach; • background of the incident, timelines, and a chronology of events; • description of the personal health information involved and affected individuals; • description of the investigative process; • the root and contributing causes of the incident; • a review of applicable legislation, safeguards, policies, and procedures;

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
	webmaster@oipc.sk.ca (The Office is paperless and prefers electronic communication.)		reports it to the IPC."		• a summary of possible solutions and recommendations for preventing future breaches. This should include specific timelines and responsibility for implementation of each action.
	Individuals	Guidance from the OIPC states it is best practice to notify affected individuals in most cases.	Guidance states that notification to individuals should occur as soon as possible after key facts about the breach have been established.	Guidance states "**It is best to contact affected individuals directly, such as by telephone, letter or in person.** However, there may be circumstances where it is not possible and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include a notice on a website, posted notices, media advisories, and advertisements. **Ensure the breach is not compounded when using indirect**	Guidance states that notifications to individuals should include the following information: • a description of the breach (a general description of what happened); • a detailed description of the personal health information involved (e.g. name, medical record, etc.); • steps taken and planned to mitigate the harm and to prevent future breaches; • if necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g. how to change a health services number); • contact information of an individual within your organization who can answer questions and provide further information; • a notice that individuals have a right to complain to the IPC (provide contact information); and • recognition of the impacts of the breach on affected individuals and an apology.

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
				notification." (emphases added)	
Manitoba *Personal Health Information Act* (PHIA) Generally speaking, PHIA applies to trustees who maintain (have custody or control of) personal health information. Trustees are: • all public bodies that fall under FIPPA; • health professionals licensed or registered to provide health care or health	**Manitoba Ombudsman – Access and Privacy Division** 750 - 500 Portage Avenue (Colony Square), Winnipeg, MB R3C 3X1 Phone: (204) 982-9130 Tolll-free: 1-800-665-0531 ombudsman@ombudsman.mb.ca	Provincial legislation requires that public bodies and trustees provide notification to Manitoba Ombudsman, when a public body or trustee determines that the privacy breach has created a real risk of significant harm for the individuals affected (FIPPA 41.1(2); PHIA 19.0.1(2)). Breach reporting is mandatory if that threshold is met. For determining if a privacy breach could reasonably be expected to create a real risk of significant harm to an individual, the relevant factors to be considered are (FIPPA regulation 3.1; PHIA regulation 8.7): (a) sensitivity of the personal information (b) probability it could cause significant harm to the individual, having regard for (i.) the event that caused the privacy breach to occur (malicious intent, theft, unauthorized access to a computer system), (ii.) number of persons who actually or potentially have access to the personal information,	If the trustee is required to notify an individual about a privacy breach, the trustee must also notify the Ombudsman at the time and in the form and manner that the Ombudsman requires (FIPPA 41.1(4); PHIA 19.0.1(4)).	Please see the Manitoba Ombudsman's Privacy Breach Reporting Form, which can be used to submit information regarding a breach to the Ombudsman directly.	The Manitoba Ombudsman has created a Privacy Breach Reporting Form that allows public bodies and trustees to complete an analysis of the nature of the breach, risk evaluation and notification steps taken. If an organization has a similar internal breach reporting form, it may submit that to the Manitoba Ombudsman in lieu of, or in addition to, their reporting form.

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
professionals (such as doctors, nurses, physiotherapists, psychologists, etc.); • health care facilities (such as hospitals, personal care homes, psychiatric facilities, medical clinics, laboratories, the Manitoba Cancer Treatment and Research Foundation, and community health centres or other health care facilities designated in the regulations); and • health services		(iii.) whether the identity of the individual with, or potential, access is known or unknown, (iv.) any known relationship and the nature of the relationship between the individual who's information has been breached and the accessor, (v.) if the public body is reasonably satisfied any unauthorized copies of the personal information have been destroyed and has committed to not use or disclose it, (vi.) the length of time since the privacy breach first occurred and the duration of the period in which the personal information was available to be accessed, used, disclosed, destroyed or altered in contravention of the Act, (vii.) the amount of personal information involved, (viii.) if the personal information has been recovered, (ix.) if the personal information adequately encrypted, anonymized otherwise not easily accessible, and (x.) if harm has materialized; and (c) any other factors that are reasonably relevant in the circumstances. The Acts define the term significant harm and provide examples of harm which can impact an individual (FIPPA 41.1(1)); PHIA 19.01(1)): • bodily harm • humiliation • damage to the individual's reputation or relationships	The Manitoba Ombudsman's Privacy Breach Reporting Form states that incidents should be reported as soon as possible even when all of the information is not yet known.		

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
agencies providing health care under an agreement with another trustee (such as the Victorian Order of Nurses and We Care).		• loss of employment, business or professional opportunities • financial loss • identity theft • negative effects on the individual's credit rating or report • damage to or loss of the individual's property Applicable guidance states a third-party entity, contracted to maintain or process personal or personal health information, should work together with the public body or trustee to determine the real risk of significant harm.			
	Individuals	Provincial legislation requires that public bodies and trustees provide notification to individuals affected by a privacy breach, when a public body or trustee determines that the privacy breach has created a real risk of significant harm for the individuals affected. Breach reporting is mandatory if that threshold is met. See above for the criteria used to determine when a breach creates "a real risk of significant harm" (FIPPA regulation 3.1; PHIA regulation 8.7). Manitoba's Ombudsman has published guidance detailing key steps in responding to privacy breaches under FIPPA and PHIA, including containment of the breach, evaluation of risks associated with the breach, and notification of affected individuals and others. A	Notice to the individual must be given as soon as practicable after the privacy breach becomes known to the head of the public body (FIPPA 41.1(3);	A mandatory notification under the Acts also requires that the notice to the individual be given directly – by telephone, letter or in person – except in specific circumstances as described in the regulations. Guidance states this method is preferred where: • the identities of individuals are known; • current contact information for the	Manitoba Ombudsman has created a practice note, Privacy Breach Notification Letter Checklist, that outlines what information to include in a notification letter to an affected individual. This includes a description of what happened, the information involved in the privacy breach, what individuals can do to lessen the impact of the breach, any corrective measures that can be taken, the steps that the public body or trustee has taken or intends to take to reduce the risk of harm, information regarding individual's right to complain, and contact information of someone who can answer individuals' questions. The notice must be given in writing and must include (FIPPA regulation 3.2; PHIA regulation 8.8): (a) a description of the circumstances of the privacy breach;

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
		key consideration in deciding whether to notify affected individuals should be whether notification is necessary to avoid or mitigate harm to an individual whose personal or personal health information has been affected by the privacy breach. Applicable guidance states notification can also be an important risk mitigation strategy in the appropriate circumstances, whether it is deemed mandatory or not.	PHIA 19.0.1(3)).	affected individuals is available; • individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach; • individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.). There are exceptions under specific circumstances where providing indirect notification – posted notices, website information or media – may be appropriate (FIPPA regulation 3.3(1); PHIA regulation 8.9(1): (a) if the trustee reasonably believes that the privacy breach may result in a risk to public health or safety; (b) if the identity or current contact information of the individual or individuals is not known (c) if the trustee reasonably believes giving notice to an individual in	(b) the date or period of time that the privacy breach occurred, or is believed to have occurred; (c) the name of the trustee who had custody or control of the personal information at the time of the privacy breach; (d) a description of the personal information that was the subject of the privacy breach; (e) a description of the steps that the trustee has taken or is intending to take, as of the date of the notice, i. to reduce the risk of harm to the individual as a result of the privacy breach, and ii. to reduce the risk of a similar privacy breach in the future; (f) a description of the steps that the individual can take to reduce the risk of harm that can result from the privacy breach or to mitigate that harm; (g) a statement that the Ombudsman has been or will be given notice of the privacy breach, as required under the Acts; (h) the name and contact information of an officer or employee of the trustee who is able to answer questions about the privacy breach; and (i) any other information that the trustee considers relevant.

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
				accordance with section 8.8 i. is impractical or unduly expensive because of the large number of individuals that may have been affected by the privacy breach, or ii. could threaten or harm the individual's mental or physical health. In circumstances where indirect notice is permitted, it must be given (FIPPA regulation 3.3(2); PHIA regulation 8.9(2): (a) by public communication or similar measure that: i. can be reasonably expected to reach the affected individual or individuals, and ii. does not include any information that could reasonably identify the affected individual or individuals, or (b) if the notice of the privacy breach can be	

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
				reasonably expected to threaten or harm the recipient's mental or physical health, notification must be provided in writing to an individual who provides care to the recipient or an individual with whom the recipient is known to have a close personal relationship.	
Nova Scotia *Personal Health Information Act* ("PHIA") Note: Generally speaking, the PHIA defines "Custodian" as an individual or organization who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties.	**Information and Privacy Commissioner** Park Lane Terraces 502-5657 Spring Garden Road Halifax, NS B3J 3R4 Phone: (902) 424-4684 No Charge-Dial: 1-866-243-1564 Fax: (902) 424-8303	OIPC guidance indicates the following factors are relevant in deciding whether or not to report a breach to the OIPC even when a notification is not required: • The sensitivity of the information – generally the more sensitive the information at risk, the more likely the Office of the Information and Privacy Commissioner for • Nova Scotia will be notified; • Whether the disclosed information could be used to commit identity theft; • Whether there is a reasonable chance of harm from the disclosure including nonpecuniary losses; • The number of people affected by the breach; • Whether the information was fully recovered without further disclosure; • Your public body, municipality or health custodian wishes to seek advice or • comment from the Information and Privacy Commissioner for Nova Scotia to aid in • managing the privacy breach; • Your public body, municipality or health custodian requires assistance in developing	In situations where the OIPC must be notified, the notification must be completed as soon as possible (PHIA s. 70) (OIPC guidance states that this should be completed "within days" whenever possible, however it is possible that notification may need to be delayed so	The OIPC has made available a Privacy Breach Report Form that may be used to report a breach.	The OIPC has made available a Privacy Breach Report Form to assist custodians with respect to the content to be included in a privacy breach report to the Commissioner.

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
	oipcns@novascotia.ca	• a procedure for responding to the privacy breach, including notification; • Your public body, municipality or health custodian is concerned that notification • may cause further harm; and/or • To ensure steps taken comply with the public body's obligations under privacy legislation.	as not to impede a criminal investigation). .		
	Individuals	A custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity (PHIA s. 69) if the custodian believes on a reasonable basis that: (a) the information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification; and (b) as a result, there is potential for harm or embarrassment to the individual (PHIA s. 69). On the other hand, where a custodian determines on a reasonable basis that personal health information has been stolen, lost or subject to unauthorized access, use, disclosure, copying or modification, but (a) it is unlikely that a breach of the personal health information has occurred; or	A custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity (PHIA s. 69)	OIPC guidance indicates that direct notification to individuals is preferred – whether by phone, letter or in person. Indirect notification – via websites, posted notices or media reports – should generally only occur in rare circumstances such as where direct notification could cause further harm or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.	Notifications to individuals should include the following information: • Date of the breach; • Description of the breach; • Description of the information inappropriately accessed, collected, used or disclosed; • Risk(s) to the individual caused by the breach; • The steps taken so far to control or reduce the harm; • Where there is a risk of identity theft as a result of the breach, typically the notice • should offer free credit watch protection as part of the mitigation strategy; • Further steps planned to prevent future privacy breaches; • Steps the individual can take to further mitigate the risk of harm (e.g. how to contact credit reporting agencies to set up a credit watch, information explaining how to change a personal health number or driver's licence number);

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
		(b) there is no potential for harm or embarrassment to the individual as a result, the custodian may decide that notification to the individual pursuant to is not required. In that case the custodian shall notify the OIPC as soon as possible (PHIA s. 70).			• Contact information of an individual within the public body, municipality or health organization who can answer questions or provide further information; • Information and Privacy Commissioner for Nova Scotia contact information and the fact that individuals have a right to complain to the Information and Privacy Commissioner under the Privacy Review Officer Act and PHIA; and • If the public body, municipality or health custodian has already contacted the Information and Privacy Commissioner, include this detail in the notification letter.
New Brunswick *Personal Health Information Privacy and Access Act* ("PHIPAA") Note: "Custodian" is generally defined as an individual or organization that collects, maintains or uses personal health information for the purpose of providing or assisting in the provision of health care or treatment or the planning and	**Ombud NB – Access to Information and Privacy Division** 65 Regent Street, Suite 230 Fredericton, N.B. E3B 7H8 Phone: (506) 453-5965 Toll-free: 1-877-755-2811 Fax: (506) 453-5963	A custodian must notify the Ombud and the individual affected if personal health information is stolen, lost, disposed of in a manner not permitted by legislation or disclosed to or accessed by an unauthorized person, unless the custodian reasonably believes that the theft, loss, disposition, disclosure or access of personal health information will not lead to the identification of the affected individual and will not have an adverse impact on the provision of health care or other benefits to the affected individual or on the affected individual's mental, physical, economic or social well-being (PHIPAA, s. 49).	Notice must be given at the "first reasonable opportunity" (PHIPAA, s. 49).	The Ombud has made available a Privacy Breach Report Form which may be used to report a breach.	While the Ombud has made available a Privacy Breach Report Form to assist custodians in reporting a privacy breach, notifications should include the following information: • The name of the custodian; • The name and contact information of the person designated by the custodian to respond to inquiries about the custodian's information practices; • A description of the nature of the breach of privacy; • The date and location of the breach of privacy; and • The date the breach of privacy came to the attention of the custodian (PHIPAA Reg s. 19).

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
management of the health care system or delivering a government program or service.	aip-aivp@gnb.ca				
	Individuals	See above.	See above.	Notice to individuals should be given by telephone or in writing. (PHIPAA Reg s. 19)	N/A
Newfoundland and Labrador *Personal Health Information Act* ("PHIA") Note: "Custodian" is generally defined as a person described in section 4(1) of the statute who has custody or control of personal health information as a result	**Information and Privacy Commissioner** P.O. Box 13004, Station "A" St. John's, NL A1B 3V8 Phone: (709) 729-6309 Fax: (709) 729-6500	A custodian must notify the Information and Privacy Commissioner if the custodian reasonably believes that there has been a "material breach", based on consideration of prescribed circumstances, involving the unauthorized collection, use, or disclosure of personal health information (S. 15(4)).	N/A	The Risk Management Toolkit includes a PHIA Privacy Breach Incident Report Form to assist custodians in reporting a privacy breach.	A custodian is required to have a written statement available that (1) gives the general description of the custodian's information policies and procedures, (2) sets out the name and access information of the custodian or the custodian's contact person, (3) describes how people can obtain access to or request correction of their personal health information, and (4) describes how a complaint may be made to the Privacy Commissioner.

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
of or in connection with the performance of the person's powers or duties.	commissioner@oipc.nl.ca				
	Individuals	Notification is required where an individual's health information is stolen, lost, disposed of in a manner not permitted by legislation or disclosed to or accessed by an unauthorized person, unless the custodian reasonably believes that the theft, loss, unauthorized disposition or improper disclosure of the health information will not have an adverse impact on the provision of health care or other benefits to the affected individual, or the mental, physical, economic or social well-being of the affected individual (S. 20(3)); S. 15(3)). Notification to an individual is **not** required where the custodian reasonably believes the theft/loss/disclosure will not have an adverse effect on the provision of health or other benefits to the affected individual, or the mental, physical, or social well-being of the individual (S. 15(7)).	Notice to individuals must be given at the first reasonable opportunity, except where under s. 58 the custodian would be required or permitted to refuse access to the record of personal health information (S. 20(3)).	PHIA does not specify the manner in which notification must be carried out. However, for example, notification can be by telephone or in writing, or depending on the circumstances, a notation made in the individual's file to be discussed at their next appointment; There are many factors that may need to be taken into consideration when deciding on the best form of notification (e.g., the	When notifying individuals affected by the breach, custodians should provide details of the extent of the breach and the specifics of the personal health information involved in the breach; the steps that have been or will be taken to address the breach, both immediate and long-term; that the NL OIPC has been contacted to ensure that all obligations under the Act are fulfilled, where applicable (certain circumstances actually require custodians to notify the NL OIPC about a breach – see section 15(4) of PHIA); and, that individuals may contact the NL OIPC directly if they are not satisfied with the measures taken by the custodian to respond to the breach.

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
				sensitivity of the personal health information). As a result, the health information custodian may want to contact the NL OIPC to discuss the most appropriate form of notification.	
Prince Edward Island *Health Information Act* ("HIA") Note: "Custodian" is generally defined as a person or organization that collects, maintains, uses or discloses personal health information for the purpose of providing or assisting in the provision of health care or treatment or the planning and management of the health care system or delivering a government program	**Information and Privacy Commissioner** J. Angus MacLean Building 180 Richmond Street, 2nd floor P.O. Box 2000 Charlottetown, PE C1A 7N8 Phone: 902-368-4099 Fax: 902-368-5947 InfoPrivacy@assembly.pe.ca	In the event of a privacy breach, custodians are required to notify the individual to whom the personal health information relates, and PEI's Office of the Information and Privacy Commissioner (the "Commissioner"), at the first reasonable opportunity, unless the custodian reasonably believes that the privacy breach will not have an adverse impact on: • The provision of health care; • Physical well-being; • Economic wellbeing; • Social well-being; • Mental well-being; and/or • Other benefits of the individual to whom the personal health information relates.	At the first reasonable opportunity.	Notification to the Commissioner must be in writing.	Although the contents of the notification are not prescribed by the HIA, the Commissioner provides a form on its website (www.oipc.pe.ca) to submit to the Commissioner. When completed, this form should provide the necessary background information of the privacy breach (e.g. name and contact information of custodian, date and time of breach, date breach was discovered, types of personal health information involved, etc.).

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
or service related to health care.	**Individuals**	See above.	See above.	N/A	See above. Guidance from the Commissioner notes that it is also advisable to provide an explanation of the circumstances of the breach to the individual, if possible.
Yukon Health Information Privacy and Management Act (HIPMA)	**Yukon Information and Privacy Commissioner** 3162 Third Avenue, Main Floor Whitehorse, Yukon, Y1A 1G3 Phone: 867-667-8468 Toll-free in Yukon: 1-800-661-0408 (ext. 8468) intake@yukonombudsman.ca	If a custodian is required to notify an individual of a security breach in relation to the individual's personal health information in the custodian's custody or control as a result of the factors outlined below and under section 30 of HIPMA, the custodian must, within a reasonable time after discovering the security breach, submit to a written report to the Commissioner. (HIPMA, section 31(1))	Within a reasonable time after discovering the security breach.	In writing.	The custodian must submit a written report to the Commissioner that: (a) assesses the risk of harm to individuals as a result of the security breach, and estimates the number of individuals so affected; and (b) describes the measures, if any, that the custodian has taken to reduce the risk of harm to individuals as a result of the security breach. (HIPMA, section 31(1)) The custodian must also provide the Commissioner with a copy of the notice provided to individuals, as described below. The content of the notification to the Commissioner should include information such as that requested on this form (e.g. types of personal health information affected, containment efforts, assessment of risk of harm, number of individuals affected, etc.).

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
	Individuals	If a security breach occurs in relation to an individual's personal health information in a custodian's custody or control, and there are reasonable grounds to believe that the individual is at risk of significant harm as a result of the security breach, the custodian must, as soon as reasonably possible after the security breach, notify the individual of the security breach. (HIPMA, section 30(1)) HIPMA defines breaches as a theft, loss, access, disposition, or disclosure of PHI contrary to the Act and its Regulations. In determining whether a custodian has reasonable grounds to believe that an individual is at risk of significant harm as a result of a security breach in relation to the individual's personal health information, the following are to be considered: (a) the length of time between the occurrence of the security breach and its discovery by the custodian; (b) the likelihood that there has been any disclosure, unauthorized use or copying of the personal health information; (c) the information available to the custodian regarding the individual's personal circumstances; (d) the likelihood that the personal health information could be used for the purpose of identity theft or identity fraud; (e) the number of other individuals whose personal health information is or may be similarly affected;	As soon as reasonably possible after the security breach.	N/A	In the notice to individuals, the custodian must: (i) describe the circumstances of the security breach and the personal health information involved; (ii) indicate when the security breach occurred; (iii) describe the measures, if any, that the custodian has taken to reduce the risk of harm to the individual as a result of the security breach; and (iv) identify the custodian's contact individual. (HIPMA, section 30(2))

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
		(f) the measures, if any, that the custodian took after the security breach to reduce the risk of harm to the individual as a result of the security breach; and (g) any factor that is reasonably relevant in the circumstances or is prescribed for this purpose. (HIPMA, section 30(3))			
Northwest Territories *Health Information Act* ("HIA") Note: "health information custodian" means (a) the Department, (b) a medical practitioner, other than a medical practitioner acting as an agent of a health information custodian, (c) a pharmacist as defined in subsection	**Information and Privacy Commissioner** P.O. Box 382, Yellowknife, NT, X1A 2N3 Phone: 1-867-669-0976 Toll-Free: 1-888-521-7088 admin@atipp-nt.ca	Under the HIA's regulations, a health information custodian must give notice to the Northwest Territories' Information and Privacy Commissioner (the "Commissioner") and law enforcement officials (i) if personal health information is lost or stolen, or (ii) if, through fraud or identity theft, personal health information is disclosed, altered, destroyed or otherwise disposed of. Notice to the Commissioner of an incident involving the loss or unauthorized use, destruction or alteration of personal health information is **not** required if the loss, use, destruction or alteration does not present a reasonable risk of harm to the affected individual. Guidance states that custodians should consider notification to: • affected individuals, including patients, health service providers, and custodians, as required by HIA, ATIPP, PIPEDA, and contractual obligations	While there is no statutory requirements regarding timing of notification, Guidance states that "the consequences of a breach can become much worse if it is not managed quickly."	N/A	While there is no statutory requirements regarding content to be included in the notification, Guidance states that "you might be required to fill out a Privacy Breach Incident Report". Currently, there is no such report available on the Commissioner's website.

Jurisdiction		Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
1(1) of the Pharmacy Act, other than a pharmacist acting as an agent of a health information custodian, (d) a prescribed organization responsible under the Hospital Insurance and Health and Social Services Administration Act for the management, control and operation of one or more facilities from which health services are provided, or (e) a prescribed person or class of persons, or a prescribed organization other than an organization prescribed as a health information custodian		• law enforcement if the breach involves theft or criminal activity • insurers • professional or other regulatory bodies • credit card companies and/or credit reporting agencies • IPC • GNWT Risk Management Office • GNWT Office of the Chief Information Officer • DHSS			
	Individuals	A health information custodian must give notice to an individual and, if applicable, to a prescribed person or organization, as soon as reasonably possible if personal health information about the individual is (a) used or disclosed other than as permitted by this Act; (b) lost or stolen; or (c) altered, destroyed or otherwise disposed of without authorization (section 87, HIA).	As soon as reasonably possible.	N/A	N/A

Jurisdiction	Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
Nunavut *Consolidation Of Access to Information and Protection of Privacy Act* ("ATIPP") See also the Government of Nunavut's Privacy Breach and Incident Policy **Information and Privacy Commissioner** P.O. Box 262, Yellowknife, NT, X1A 2N2 Phone: 1-867-446-8631 Toll-Free: 1-888-521-7088 admin@atipp-nu.ca	Note: The Government of Nunavut does not have legislation specific to breach notification involving personal health information. Rather, breach notification is dealt with under ATIPP and Nunavut's Privacy Breach and Incident Policy. Under section 49.8 of ATIPP, a breach of privacy occurs with respect to personal information if (a) the information is accessed and the access is not authorized under this Act; (b) the information is disclosed and the disclosure is not authorized under this Act; or (c) the information is lost and the loss may result in the information being accessed or disclosed without authority under this Act. A public body that knows or has reason to believe that a breach of privacy has occurred with respect to personal information under its control shall report the breach of privacy to the Information and Privacy Commissioner in accordance with this section if the breach is **material**. **Material breach of privacy – factors** The factors that are relevant in determining whether a breach of privacy with respect to personal information under the control of a public body is material include (a) the sensitivity of the personal information; (b) the number of individuals whose personal information is involved;	The report to the Commissioner must be made as soon as reasonably possible after the public body knows or has reason to believe that the breach of privacy occurred and determines that the breach is material. The notice to individuals must be given as soon as reasonably possible after the public body knows or has reason to believe that the breach of privacy occurred and determines that the breach of privacy creates a real	N/A	The notice to individuals must contain (a) sufficient information to allow the individual to (i) understand the significance to him or her of the breach of privacy, and (ii) take steps, if any are possible, to reduce the risk of, or mitigate, any harm to him or her that could result from the breach of privacy; (b) information describing what steps the public body has taken to reduce the risk of, or mitigate, any harm to the individual that could result from the breach of privacy; and (c) such other information as may be prescribed. The report to the Commissioner must describe the steps taken by the public body to comply with sections 49.10 and 49.11 of ATIPP and must contain such other information as may be prescribed.

Jurisdiction	Notification Threshold	Timing of Notification	Method/ Manner of Notification	Content of Notification
	(c) the likelihood of harm to the individuals whose personal information is involved; and (d) an assessment by the public body whether the cause of the breach is a systemic problem. (ATIPP, section 49.9) A public body that knows or has reason to believe that a breach of privacy has occurred with respect to an individual's personal information under the public body's control shall notify the **individual** of the breach of privacy in accordance with this section if it is reasonable in the circumstances to believe that the breach of privacy creates a real risk of significant harm to the individual. (ATIPP, section 49.10) **Real risk of significant harm – factors** The factors that are relevant to determining whether a breach of privacy with respect to an individual's personal information creates a real risk of significant harm to the individual include (a) the sensitivity of the personal information; and (b) the probability that the personal information has been, is being or will be misused.	risk of significant harm to the individual.		