International Data Privacy Day 2018 – Protecting your personal information

Privacy laws are in place to safeguard your personal information and protect you. We marked International Data Privacy Day this year on January 28th, and as your Privacy Commissioner, I want to highlight the steps being taken around the world to enhance the protection of citizens' personal information. In Canada, every jurisdiction has privacy laws that protect the personal information of citizens and has privacy commissioners responsible for monitoring compliance. Most other countries also have privacy laws and privacy commissioners. The need to enhance privacy protection is now greater than ever, due to advances in technology. Governments and businesses are able to collect massive amounts of personal information, which can be easily processed, transmitted and breached.

Privacy laws allow individuals to control their own personal information. These laws impose limits on the collection, use and disclosure of personal information by governments and businesses. They also require governments and businesses to properly secure personal information so that breaches do not occur.

A privacy breach can cause harm to an individual. In recognition of these risks, most newly-drafted privacy laws include a requirement that governments and businesses notify individuals about a breach that may cause them harm. There is also usually a requirement that privacy commissioners be informed about the breach. Existing privacy laws are being amended to include breach reporting.

The purpose of breach reporting is to ensure individuals know about a breach so they may take steps to prevent any potential harm. It is also to ensure privacy commissioners can monitor breaches and help with prevention.

What are privacy breach reporting requirements in Yukon?

Health care providers in the Yukon public and private sectors are required to comply with the *Health Information Privacy and Management Act* (HIPMA). HIPMA requires reporting of any breaches. A health care provider must notify individuals following a privacy breach where there is a risk of significant harm to the individuals, and Yukon's Privacy Commissioner must also be informed. If found guilty of failing to notify an individual under HIPMA, the fines are between $10,000 and $100,000.

The *Access to Information and Protection of Privacy Act* (ATIPP Act), which has been in effect in Yukon since 1995, applies to public bodies, including the Yukon government. The ATIPP Act does not have mandatory breach reporting requirements, but they may be included when the legislation is amended following a comprehensive review currently underway.

There are also privacy laws which govern the private sector. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is federal privacy law that applies to the collection, use and disclosure of personal information by an organization in the course of commercial activity. It applies to all private sector organizations in Yukon, including private sector health care providers. It also applies to federal works, undertakings or businesses including banks and telecommunications and transportation companies. PIPEDA was recently amended to include mandatory breach reporting. The amendments have not yet come into force but now that the regulations are drafted, it's only a matter of time. Once in effect, the requirement to notify an individual (and the federal Privacy Commissioner) about a breach will be triggered when an organization determines the breach creates a real risk of significant harm to the individual. Failure to report a breach is an offence subject to fines similar to those in HIPMA.

The *General Data Protection Regulation* (GDPR) is a European Union (EU) law that includes mandatory breach reporting requirements. It will come into effect in May 2018. This law is said to have "extra territorial" reach because it will apply to an organization that collects, uses or discloses personal information of EU citizens while offering goods or services to them or monitoring their behavior, no

matter where the organization is located. Since EU residents visit Yukon every year, it is possible that Yukon businesses may find themselves subject to the GDPR.

The GDPR requires organizations to notify the appropriate supervisory authority within 72 hours about a breach of personal information. An organization must notify individuals affected by a breach without undue delay when the breach is likely to result in a high risk to their rights and freedoms.

A supervisory authority is similar to a privacy commissioner in Canada. The appropriate supervisory authority would be the authority in the country where the citizen affected by the breach resides. Supervisory authorities have the power to impose an administrative fine on an organization that fails to comply with the GDPR's breach reporting requirements. The fines can be up to 10 million euros or 2 per cent of the organization's global turnover (whichever is higher).

Ensuring compliance

The best way for public or private sector organizations to avoid being found in violation of mandatory breach reporting requirements is to identify a "privacy contact", i.e. someone in the organization to be responsible for privacy and to develop breach reporting policy and procedure. All staff need to be trained on the policy and procedure, so that they know what a privacy breach is and who to call when one is discovered. The policy should require employees to notify the organization's privacy contact immediately upon learning of a breach. The privacy contact must be trained on how to effectively manage a breach and on the mandatory breach reporting requirements in applicable laws.

It is for the benefit of all Yukoners and businesses alike if privacy laws are understood and followed so that breaches are avoided!

Privacy breach reporting requirements chart

This chart sets out privacy laws in Yukon and their breach reporting requirements, to help businesses and organizations understand the requirements and determine if they are subject to them.

Note: PC means Privacy Commissioner and SA means Supervisory Authority

Applicable Law	**HIPMA – Yukon Law** **(In force)**	**PIPEDA – Federal Law** **(Breach reporting not yet in force)**	**GDPR – EU Law** **(In force May 2018)**
Who it applies to	<u>Custodians</u> Includes: • Minister of Health • Department of Health & Social Services • Operator of a hospital such as Yukon Hospital	<u>Organizations</u> That collect, use or disclose personal information in the course of a commercial activity Includes: • retail businesses operating in Yukon	<u>Controllers</u> The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

	Corporation or a health facility • A health care provider including medical practitioners, registered nurses or nurse practitioners, LPNs, pharmacists, chiropractors, optometrists, dentists, dental assistants, dental therapists, dental hygienists, and denturists) • Kwanlin Dun First Nation Health Centre • EMS in the Department of Community Services • Many Rivers Counselling and Support Services Society • Child Development Centre	• private sector health care providers operating in Yukon	Includes: • any public or private sector organization in Yukon that processes the personal data of individuals in the EU or that monitors their activity <u>Processers</u> A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Includes: • any public or private sector organization in Yukon that processes personal data on behalf of a controller
Trigger for notification of individuals	30 (1) An individual must be notified about a breach of personal health information when the custodian has reasonable grounds to believe that the individual is at risk of significant harm from the breach	10.1 (3) An individual shall be notified of any security breach if it is reasonable in the circumstances to believe the breach creates a real risk of significant harm to the individual	Article 34, 1 When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject
Timing for notification of individuals	30 (1) As soon as reasonably possible after the security breach	10.1 (6) As soon as feasible after the organization determines a breach has occurred	Article 34, 1 Without undue delay

Oversight authority breach reporting requirements	30 (2)(b) A copy of the notice to individuals must be provided to the PC at the same time it is provided to individuals 31 (1) Report about the breach must be submitted to the PC within a reasonable time after the breach containing the information specified in paragraphs 31 (1)(a)&(b)	10.1 (1) Report about the breach shall be reported to the PC if it is reasonable in the circumstances to believe the breach will result in a real risk of significant harm to an individual 10.1 (6) Report must be provided to the PC as soon as feasible after the organization determines a breach has occurred	Article 33, 1 The controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the SA Note that there is a requirement that processors notify the controller without undue delay after becoming aware of a personal data breach
Offence	121 (1)(g) A person is guilty of an offence if the person knowingly contravenes subsection 30 (1) 121 (2) A person is guilty of an offence if they knowingly contravene HIPMA	28 An organization is guilty of an offence if it knowingly violates subsection 10.1 (1)	Article 83 establishes administrative fines that may be imposed by SAs
Penalty	121 (1)(g) $25,000 for an individual and for all other cases $100,000 121 (2) $500	28 (a)&(b) $10,000 on summary conviction or $100,000 on an indictable offence	Article 83, 4 Administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher