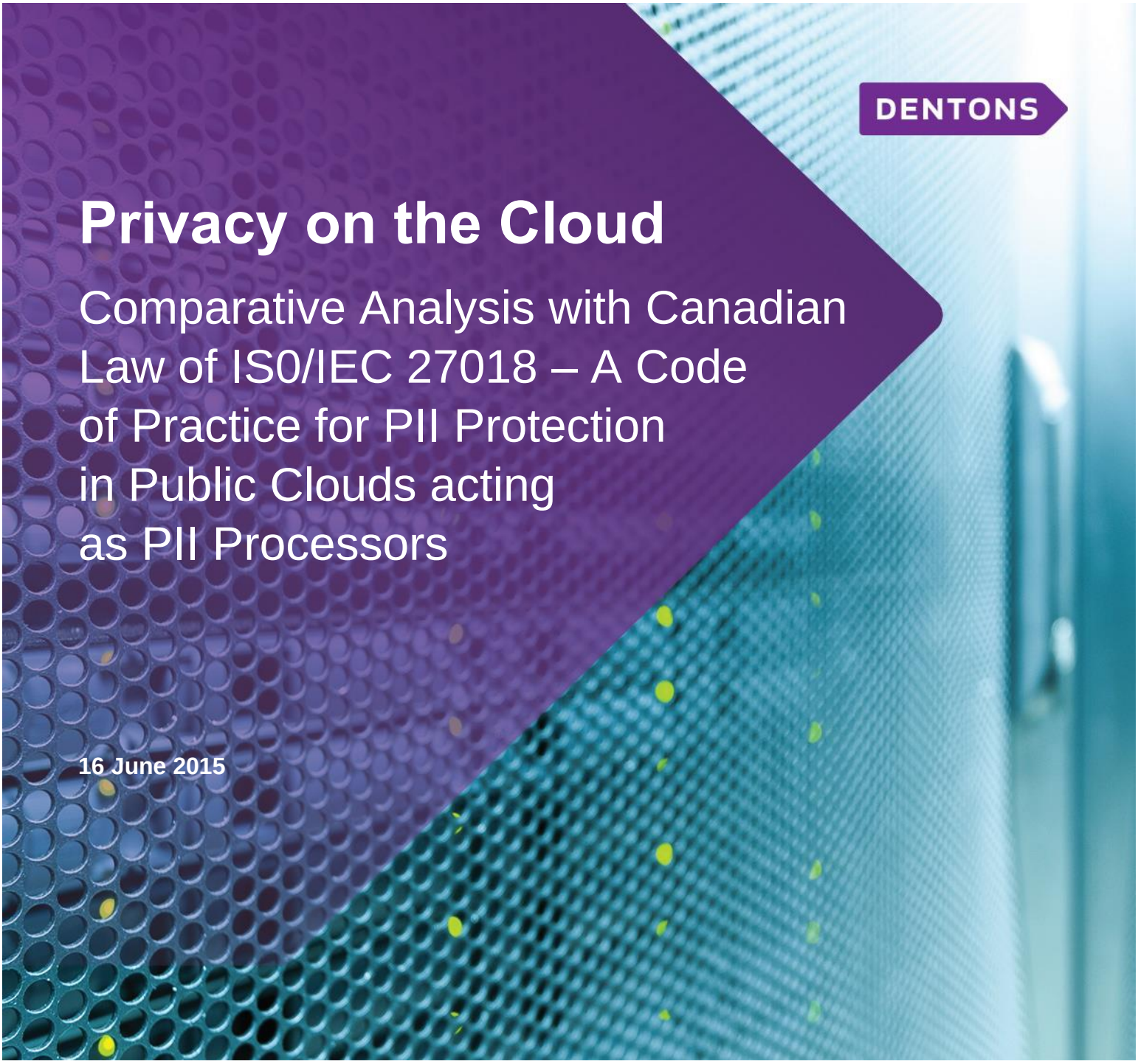

Privacy on the Cloud

Comparative Analysis with Canadian Law of IS0/IEC 27018 – A Code of Practice for PII Protection in Public Clouds acting as PII Processors

16 June 2015

Contact

Chantal Bernier
Dentons Canada LLP
1420–99 Bank Street
Ottawa, ON K1P 1H4

chantal.bernier@dentons.com
D +1 613 783 9684
T +1 613 783 9600
F +1 613 783 9690

Comparative Analysis with Canadian Law of ISO/IEC 27018 – A Code of Practice for PII Protection in Public Clouds acting as PII Processors

Foreword

Understanding the Standard

ISO/IEC 27018 is the international Code of Practice for Personal Identification Information (PII) protection in public clouds acting as PII processors, adopted on April 25, 2014.

The Office of the Privacy Commissioner of Canada – with input from representatives of the Government of Canada, other States and Data Protection Authorities – has significantly contributed to the development of the Standard.

About ISO and IEC

ISO/IEC 27018 describes ISO and IEC processes as follows:

> *ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.*
>
> *International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.*
>
> *The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.*
>
> *Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.*
>
> *ISO/IEC 27018 was prepared by* Joint Technical Committee *ISO/IEC JTC 1,* Information technology, Subcommittee *SC 27, Security techniques.*

Contents

I General Application

Recent news that Microsoft has received certification for compliance with ISO/IEC 27018, an International Standard with a *Code of practice for PII protection in public clouds acting as PII processors,* prompts exploration of the meaning of this development, particularly for the holders of the most voluminous and sensitive personal data bases: public bodies.

The certification of Microsoft comes from the British Standards Institution, an independent auditor, on the basis of Microsoft's incorporation of the controls and best practices of ISO/IEC 27018 into Microsoft Azure, Office 365 and Dynamics CRM Online.

It seems that Microsoft is, so far, the first major cloud service provider to receive this certification.

The question is whether this development will bring Canadian public bodies to finally seize the opportunities of the cloud, including lower costs and higher data security, with the new assurance of protection of data sovereignty over the cloud.

Searching for an answer takes us from a broad description of the state of Canadian law in regard to the cloud, the benefits of the cloud, the concerns about the cloud, the comparative analysis of ISO/IEC 27018 Standard with Canadian privacy law and the best practices that emerge.

1. Overview of Canadian law on the cloud

No law in Canada specifically prohibits or regulates the storage of personal information on the cloud. However, public bodies in general are concerned about possible loss of data control on the cloud and loss of data sovereignty on foreign clouds.

British Columbia and Nova Scotia have both adopted legislation that prohibits public bodies from storing and accessing information outside Canada.[1] Since 90% of Canadian Internet traffic goes through the US, and the top ten ranked cloud providers are all foreign, mainly in the US[2], this, in effect, practically bars public bodies in those provinces from using cloud computing. This restriction, however, may be circumvented with consent.[3] In 2009, the BC government submitted to a special legislative committee the disadvantage of this rule and the committee acknowledged the challenges it poses.[4]

---

[1] British Columbia *Freedom of Information and Protection of Privacy Act,* RSBC 1996, c 165, s 30.1;
Nova Scotia *Personal Information International Disclosure Protection Act 2006*, SNS 2006, c 3, s 5.

[2] Talkin'Cloud 100: 2014 Edition Ranked 1 to 25, online: http://talkincloud.com/TC100/talkin-cloud-100-2014-edition-ranked-1-25.

[3] In *Mission School District No. 75*, the Information and Privacy Commissioner of British Columbia found "click to agree" sufficient to engage meaningful consent and allow storage of personal data outside Canada. *The Board of Education of School District No. 75 (Mission)*, Order F07-10 Office of the Information and Privacy Commissioner for British Columbia, 26 June 2007, online: https://www.oipc.bc.ca/orders/912.

[4] *Cloud Computing Guidelines for Public Bodies,* Office of the Information and Privacy Commissioner of British Columbia, updated June 2012, at 3, online: https://www.oipc.bc.ca/guidance-documents/1427.

Quebec privacy legislation provides that, before entrusting personal information to an enterprise outside Quebec, a public body must ensure that the information receives protection equivalent to that afforded under Quebec law.[5] Under personal health information legislation in Canada, generally, a cloud provider would be a "health information network provider" and would come under the same obligations as other processors.[6]

Reluctance of the public sector towards cloud computing has not been raised in relation to technological safeguards but to legal compliance assurance. This, consequently, is the value of ISO/IEC Standard 27018. A comparative analysis of the Standard and Canadian privacy law in the public sector, both federal and provincial, shows that the Standard meets or exceeds the requirements of Canadian law. In addition, the Standard clearly delineates the responsibilities of the cloud provider and the cloud customer, keeping the latter in full control. The breakthrough is that ISO/IEC 27018 brings the highest level of privacy compliance to the highest level of data security.

2. Working definitions

ISO defines cloud computing as "the method of distribution of aggregated services that are provided over the Internet".[7] The International Telecommunications Union foresees that: "In the future, governments, companies and individuals will increasingly turn to the cloud."[8]

ISO and IEC: the International Organisation for Standardization and the International Electrotechnical Commission form the worldwide system for standardization. They are composed of national bodies to develop international standards through technical committees.[9]

Standard ISO/IEC 27018, entitled a *Code of practice for PII protection in public clouds acting as PII processors,* was developed by the Joint Technical Committee with the following objectives: i) help public cloud providers comply with legal obligations when acting as cloud processors; ii) enable personal identifiable information (PII) cloud processors to be transparent; iii) assist cloud service customers and cloud providers to enter into contractual agreements; iv) provide cloud customers with a mechanism to exercise audit and compliance rights on the cloud.[10]

Cloud provider as cloud personal identifiable information (PII) processor is defined in ISO/IEC 27018 when it processes PII for and according to the instructions of a cloud service customer.[11]

3. The benefits of cloud computing

The Office of the Privacy Commissioner of Canada (OPC) identifies the main benefits of cloud computing as:

---

[5] *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information,* c A-2.1, s 70.1.
[6] For example, *Personal Health Information Regulations* (Ontario) O Reg 329/04, s 6(2).
[7] ISO 27000 *Certification of Cloud Computing Service.*
[8] 'Privacy in Cloud Computing', ITU-T, *Technology Watch Report*, March 2012, at 1.
[9] *Code of practice for PII protection in public clouds acting as PII processors*, ISO/IEC Standard 27018, at vi.
[10] *Ibid* at vii.
[11] *Ibid.*

i) scalability, by offering unlimited storage and processing capacity;

ii) reliability, since it eliminates the risk of losing paper, laptops or hard drives and allows access to documents and applications via Internet worldwide;

iii) cost savings, since resources are pooled for optimal safeguards thus eliminating the need for investment in infrastructure;

iv) efficiency, as the freeing up of resources through the pooling of expertise allows focus on other priorities; and

v) access to new technology as the cloud providers, being more resourceful and specialised in the area, are in a position to offer a much wider choice.[12]

Experts underline the low cost of cloud computing and world wide availability.[13]

4. The lingering concerns about the cloud

An overview of the literature on cloud computing whether from public bodies or privacy advocates brings out the following common concerns:

i) Jurisdictional complexity that mires accountability and remedy;

ii) Loss of data sovereignty for public bodies through foreign cloud providers - including data mining and access by foreign law enforcement authorities;

iii) Compromise of meaningful consent through lack of transparency;

iv) Challenge to safeguards from transfer of information across the Internet

5. The breakthrough of ISO/IEC Standard 27018

The following paragraphs address these concerns through a comparative analysis of Canadian privacy law with ISO/IEC Standard 27018.

a. Accountability and jurisdiction over the cloud

Public institutions are fundamentally accountable to Parliament through their ministers. This general accountability framework extends to privacy, as to every other legislated obligation.

In the federal public sector, specific accountability for privacy protection is addressed in section 72 of the *Privacy Act.* It states that the head of every government institution must submit to Parliament an annual report on the administration of the *Privacy Act* in that institution.[14]

[12] *Report on 2010 OPC Consultations on Online Tracking, Profiling and Targeting and Cloud Computing*, May 2011, online: https://www.priv.gc.ca/resource/consultations/report_201105_e.pdf.
[13] ITU-T Privacy in Cloud Computing, Technology Watch Report, March 2012; Martin PJ Kratz, *Canada's Internet Law in a Nutshell* (Carswell, 2013) at 488.
[14] *Privacy Act,* RSC 1985, c P-21, s 72.

The Treasury Board Secretariat of Canada Guidance Document on Privacy and Outsourcing[15] confirms that the head of a federal institution remains responsible and accountable for personal information shared with contractors through outsourcing, as cloud computing would be. Specifically, the head of an institution must ensure that contractors meet the requirements of the *Privacy Act,* develop contractual clauses to that effect and exercise monitoring to ensure compliance with those.[16] The issue of jurisdiction is clarified in that Canadian norms for privacy protection extend to contracted cloud providers.

The issue of accountability and jurisdiction is addressed by ISO/IEC Standard for compliance assurance from the cloud provider to the cloud customer: the cloud provider undertakes to assist the cloud customer to fulfill its legal obligations for privacy protection.

b. Data sovereignty over the cloud, including data mining and access by law enforcement authorities

Compliance assurance, and therefore respect for data sovereignty as well as prohibition for data mining independent from the customer, resides in the obligation, under ISO/IEC 27018, for the cloud provider to operate the cloud to meet the requirements of legislation applicable to each cloud customer. Moreover, the cloud provider must act only upon the instructions of the cloud customer. Even more to the point,

> Note that the cloud service customer has authority over the processing and use of the data. (...).Maintaining the distinction between the PII Controller (cloud customer) and the PII Processor relies on the public cloud PII Processor having no data processing objectives other than those set by the cloud service customer with respect to the PII processes and the operations necessary to achieve the cloud service customer's objectives.[17]

In particular, the Standard dictates that,

- Information security policies should be augmented by a statement committing cloud providers to compliance with applicable privacy protection (as required by Canadian law).
- Contractual agreements should clearly allocate responsibility between the cloud provider, its sub-contractors and the cloud service customer (a higher standard than Canadian law).
- The cloud provider shall promptly notify the cloud customer of a data breach as part of the contract (unspecified in Canadian law).
- A mechanism must be established by contract to ensure the cloud provider manages internal compliance with privacy protection laws of the cloud provider (a higher standard than Canadian law).
- Contract measures must be developed to ensure the personal data is not processed in any manner other than according to the instructions of the cloud customer (ensuring data sovereignty) and excluding data mining.

[15] Treasury Board of Canada Guidance Documents, 'Taking Privacy into account before making contracting decisions', 25 August 2010, online: http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp02-eng.asp.
[16] *Ibid* paras 6.2-6.3.
[17] ISO/IEC 27018, *supra* note 9 at vii.

- The cloud provider must disclose to the cloud customer the geo-location in which the personal data may be stored (higher standard than Canadian law).

The underlying objective of these provisions is that the cloud provider act strictly upon the instructions of the cloud customer. As a result, the cloud customer retains data control and data sovereignty through transfer to the cloud, while benefiting from the enhanced security of the cloud.

Specifically with respect to access by foreign law enforcement authorities to personal information held on the cloud, a concern significantly made acute since the Edward Snowden revelations, the standard states that:

- Cloud providers will reject any request for disclosure that is not legally binding and will consult the cloud customer before making any disclosure (more specific than Canadian law).

Lingering concerns that American law enforcement and national security authorities would access such data through a back door without ever requesting the information should be alleviated by American cloud providers' reaction to the Snowden revelations in this regard: they are building an infrastructure that is becoming hermetic to such intrusions. In fact, the concern of the American law enforcement authorities is that the US cloud providers have now erected a technological infrastructure that is so impenetrable to defeat even a legal warrant.

Clearly, the American cloud providers business interests have become our greatest ally in shielding our personal information as a matter of client service, competitive advantage and, yes, principle.

c. Safeguards

The obligation of public bodies to ensure security of personal information in Canadian law is either indirect, through the prohibition to disclose without consent, except in certain specified circumstances,[18] or direct in Quebec, with the obligation for public bodies to protect personal information with security safeguards appropriate to the level of sensitivity of the information.[19] ISO/IEC 27018 augments Canadian legal requirements with security standards of a higher level of specificity, such as obliging cloud providers to,

- Never process the data for any other use independent from the instructions of the cloud customer;
- Encrypt PII transmitted over public data transmission networks;
- Implement contracts with sub-contractors that specify security measures to protect data;
- Notify promptly of any data breach;
- Implement human resource security measures, access controls, physical security, operations security, and information security incident management.

In fact, the cloud provider, under ISO/IEC 27018, is obliged to support and manage compliance with privacy law for the cloud customer.

[18] *Privacy Act, supra* note 14 s 8.
[19] *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, supra* note 5 s 63.1.

d. Openness and consent

As mentioned above, a concern raised about the cloud relates to the validity of consent in the complex, and consequently opaque, world of cloud computing. In this regard, ISO/IEC 27018 lifts the veil by stating the exact modalities of cloud computing and by obliging cloud providers to their own obligation of transparency. In particular, in addition to adding openness by stating the respective obligations of cloud providers and cloud customers, ISO/IEC 27018 commits cloud providers to:

- Ensure transparency and provide PII controllers (customers) with information about their policies and practices (a higher standard than Canadian law).
- Specify the geo-location of where the PII may be stored (A non-existing norm in Canadian law).
- Notify promptly the cloud customer of a breach (unspecified in Canadian law).
- Provide the cloud customers the means to fulfill their obligation to facilitate the exercise of individuals' right to access or correction of their personal information (a non-existing standard in Canadian law).

The continuity of legal protection of PII through the ISO/IEC standard begs the question as to the necessity of any independent consent: since the privacy policies of the cloud customer must be fully respected by the cloud provider (if nothing else, for fear of losing business), the resort to the cloud is an ordinary transfer to a third party processor as is the case for so many other outsourcing contracts. Agreement to the privacy policy of the cloud customer stands for consent to outsourcing on the cloud. At most, public bodies that have no restriction on the location of data storage and access could simply inform individuals of cloud computing in their privacy policy. Public bodies in jurisdictions that do, such as British Columbia and Nova Scotia, can avail themselves of the cloud through a “click to agree” as consent.

Conclusion – Best practices and questions for public bodies to ask cloud providers

The BC Information and Privacy Commissioner,[20] various authors, and Microsoft have identified best practices for public bodies on the cloud. They may be summarised in five main points:

- While cloud computing offers every cloud customer lower costs and increased efficiencies for IT infrastructure, for public bodies it also adds the advantage of improving transparency, advance collaboration, better focus on critical needs and increase citizen’s services. In addition, the cloud offers opportunities of tailored solutions, integrated solutions and more secure data storage and access controls.
- Public bodies are encouraged to triage the data to be stored on the cloud according to sensitivity to select whether to allow data to be stored in clear text, or encryption. That being said, ISO/IEC 27018 provides for encryption of PII transmitted over public data transmission networks.
- Public bodies usually have significant existing investments in infrastructure. It is recommended that they first assess their needs, and then triage the data for what they choose to keep on their servers and what they want to store in the cloud.

[20] *Cloud Computing Guidelines for Public Bodies, supra* note 4.

- Public bodies are also encouraged to adopt ISO/IEC 27108 to narrow the eligibility of cloud providers to those that are ISO/IEC 27108 certified. This ensures that the data will be used and processed exclusively according to their instructions, will not be disclosed to law enforcement agencies or to anyone else except under lawful authority and in consultation with the cloud provider, and will receive the highest level of security.
- For those jurisdictions where public bodies cannot store data outside Canada without consent, a "click-to-agree" constitutes consent provided that it meets other, generally applicable, legal requirements.[21]

Looking at Canadian privacy law, the following questions would underpin due diligence by a public body to store data on the cloud, including a foreign cloud:

- Is the cloud provider certified under ISO/IEC 27018?
- What is the history of data security of the cloud provider?
- How does the cloud complement the existing information technology infrastructure?
- What data should go on the cloud?
- Are citizens properly informed of storage on the cloud?
- For public bodies that are prohibited from using the cloud without consent, is the consent form compliant with legal requirements?

The issues that have become non-issues with Standard ISO/IEC 27018:

- Data mining: ISO/IEC prohibits the use or processing of the data stored for the cloud customer in any manner independent of the objectives of the cloud customer or in any way separate from its instructions.
- Appropriation of data: it has been raised that cloud providers should be held to store the data "in trust". That is precisely the effect of ISO/IEC 27018: the cloud customer remains entirely in control of the data stored on the cloud and a reputable cloud provider will afford it the highest levels of security.
- Disclosure without consent: even before the revelations of Edward Snowden, the US cloud was heavy with suspicion of accessibility by US law enforcement authorities. In reality, the impact of the US *Patriot Act* is negligible – it is mainly procedural rather than substantive – and the sharing of information between Canadian and American law enforcement agencies occurs without any need of the cloud. Moreover, ISO/IEC 27018 constrains cloud providers to deny any request for personal information from law enforcement authorities without consent unless there is legally binding authority and even then will consult with the cloud customer.
- Retention of data beyond cloud computing contract: as ISO/IEC 27018 certified cloud providers do not process or use data in any manner independent from the objectives or the instructions of the cloud customer, it follows that they cannot retain data beyond the period where the cloud customer has entrusted the data to them. Specifically, ISO/IEC 27918 specifies that cloud providers will commit to erasure of temporary files and disposal of the data within contractual set times with the data customer.

[21] *Ibid* at 4.

As we examine cloud computing services through the objectives of data sovereignty and security for public bodies, the reluctance should turn to adherence. Through the main cloud service providers, cloud computing represents the most secure method for data storage and ISO/IEC 27018 elevates protection for data sovereignty to unprecedented standards. Hence, the technological robustness of the cloud is now met by equally robust norms for data protection compliance.

The result is that as 2014, dubbed “the year of the breach”, has just drawn to a close, an unprecedented level of protection emerges. The advent of an international norm that certifies the highest level of compliance for privacy protection brings that protection to the most advanced technological infrastructure to secure personal information.

II Specific Issues

The main arguments and counter-arguments around the ISO/IEC Standard 27018 on privacy in the cloud relate to:

- US clouds and NSA surveillance;
- Incentives and disincentives for cloud providers to decline law enforcement access requests;
- The value of contractual obligations to protect data;
- Ensuring compliance by cloud providers;
- The impact of ISO/IEC 27018 on data processing contract negotiations; and
- The clarification of jurisdiction over the cloud.

I will address each individually.

1. ISO/IEC 27018 and protection from NSA surveillance

The June 5th, 2014 Snowden revelations of NSA's long reach and huge appetite for personal data have profoundly undermined the world's confidence in US data processors. It did not help that on June 6th, the American government's precipitated damage control efforts were to insist that its surveillance only targeted foreigners. I was at an international privacy law conference in Columbia that day, full of what the US would call "foreigners". I can tell you it did not go down well. And the repercussions are still reverberating. Hence, the lingering doubts, even with ISO/IEC Standard 27018, towards cloud providers based in the US.

But as more Snowden revelations continue to seep, we now find out that data residency is irrelevant: the front page of the Globe and Mail of March 17, 2015 reveals that the NSA was mapping the internal communications traffic of two large Canadian companies, apparently unbeknownst to them.[22]

So the perception of safety of data in Canada must be challenged. The reality of the cloud's advantages remains.

The challenge has become one of risk management to protect privacy. What is the greatest risk to individuals: exposure to financial or reputational loss through data breaches due to inadequate safeguards for lack of resources and expertise, or damage from NSA broad surveillance? Without downplaying the gravity of the latter in terms of risk to democracy, I believe the former to be the greatest risk on the basis of reality of incidents. It also offers the greatest potential for safeguards.

Particularly since the increase in home grown terrorism and radicalization, States are "legislating up", extending their surveillance powers everywhere. It is not legitimate until justification is empirically demonstrated – still wholly wanting – but it is upon us, wherever the data are held. We must, therefore,

[22] Colin Freeze and Christine Dobby, "NSA trying to map Rogers, RBC communications traffic, leak shows", *The Globe and Mail*, 17 March 2015.

examine the value of cloud computing against the benchmarks of data security from breaches and loss, and from law enforcement or national security specific requests for access.

In relation to data security, whether in relation to breach or loss, these are the general safeguards mandated by ISO/IEC 27018, in relation to key issues:

- Policies: responsibilities must be clearly delineated between the cloud processor, the sub-contractors and the cloud customer;
- Human resources: security measures must cover recruitment, employment and post-employment, and provide for education and training as well as disciplinary processes as necessary;
- Physical and environmental safeguards: areas, equipment, cables and screens must be secure according to the highest level of protection and sensitivity of the data;
- Technology: security measures are mandated whether relating to back-ups, portable devices or malware, and technical vulnerability management.

With respect to law enforcement access requests, ISO/IEC 27018 introduces the specific commitment for the cloud provider to,

- Notify the cloud customer of any legally binding request for disclosure of personal information "unless such a disclosure is prohibited" such as the prohibition under criminal law to reveal the existence of a lawful access request to preserve the confidentiality of a law enforcement investigation;
- Reject any request for personal information that is not legally binding;
- Consult the cloud service customer "where legally permissible" before making any disclosure.

For all the improvements of ISO/IEC 27018, the application of "gag orders" in the US was brought up in the assessment of the value of the Standard. I believe the limitations placed upon cloud providers are, for all intents and purposes, universal. At least, under ISO/IEC 27018, discipline is brought around the issue: a certified cloud provider will refuse access where there is no lawful authority for the request, or will comply and consult if there is lawful authority, or will comply without consulting if it is prohibited by law. It is better than the covert, cross-border, haphazard access we now learn of.

This leads to the second main issue raised around ISO/IEC 27018: what are the incentives or disincentives for the cloud provider to disclose to authorities? The question leads us to the broader issue of compliance and the strength of contractual obligations.

2. The strengths and weaknesses of contractual obligations

It has been suggested that ISO/IEC 27018 is "an agreement to agree." Indeed, the introductory paragraphs of the Standard describe its intention as that "to create a common set of security categories and controls that may be implemented by a public cloud computing service provider acting as a PII processor".

So ISO/IEC 27018 proposes a Standard which: i) constitutes the basis for independent certification, which can be revoked for failure to comply; and ii) raises contractual obligations to the highest, universal contractual clauses.

The question remains as to the incentives or disincentives to comply with these contractual clauses. It seems fair to speculate that:

- A cloud provider that has made the significant investment to bring its operations in line with ISO/IEC 27018 to obtain certification, and whose business rests upon that certification, will not want to risk revocation of the certification (which I will address under compliance measures);
- All accountability models, whether EU Directive Standard Clauses for Data Transfers or the Canadian accountability principle, rest upon contractual clauses, with compliance mechanisms inherent to contracts. ISO/IEC 27018 raises the stakes: derogation to a cloud providing contract by an ISO/IEC 27018 certified cloud provider carries both the risk of contractual penalties and of either failing an audit and being imposed corrective measures, or losing certification.
- In relation to accepting or denying access to law enforcement authorities, boundaries, both organisational and territorial, are vanishing to the point of making the requirement for data residency superfluous. Still, ISO/IEC 27018 defines the obligations of the cloud provider in protecting personal information from unlawful access at the risk of being found in violation of both contractual clauses and certification requirements.

3. Ensuring compliance by cloud providers

The issue of incentives and disincentives to comply with the Standard leads to the issue of compliance assurance. The question must be addressed both in relation to the normative text of the Standard and to the certification process.

Within the Standard itself, the compliance provisions feature:

- Designation by the cloud provider of a contact person regarding the implementation of the contract;
- Reference to contractual sanctions in domestic law for breach of contract under the Standard; and
- Mandatory event logging and logging monitoring by the cloud provider with a “specified, documented periodicity to identify irregularities and purpose remediation efforts”.

Perhaps most importantly:

- Cloud service customers may perform audits or, should audits be impractical, require from the cloud provider “independent evidence that information security is implemented and operated“, including by way of an independent audit, chosen by the cloud provider, subject to sufficient transparency; and
- Cloud service providers must notify promptly the cloud customer in the event of an unauthorized access to personal information or to processing equipment resulting in loss, disclosure or alteration of the information.

In addition to these norms, the ISO certification process itself constitutes a measure for compliance.

ISO certification is issued by an accredited certification body upon assessment of an organisation in relation to the specific standard to which certification of compliance is sought.

When certification is issued, it is subject to scheduled audits. Where auditors find compliance issues, either corrective action is mandated or certification is revoked. Moreover, should an incident occur that reveals noncompliance with an ISO standard, even outside of an audit, certification may not be invoked to mitigate liability.

4. The impact of ISO/IEC 27018 on contract negotiations for data processing

The drafters of the ISO/IEC Standard 27018, including representatives from data protection authorities, States and private sector organisations, describe their objectives in relation to impact of the Standard as: i) assisting cloud providers in complying with privacy law; ii) fostering transparency on their part; iii) facilitating cloud service contractual agreements and; iv) providing cloud customers with a mechanisms to exercise audit and compliance rights.

It is reasonable to expect an increase in cloud service agreements with the assurances of ISO/IEC Standard 27018 and a focus on either ISO/IEC 27018 certified cloud providers or contracts based on the Standard.

The outstanding question is: will ISO/IEC 27018, entirely premised on the cloud service customer's control over the data on the cloud, make public bodies move to the higher security and cost efficiency of the cloud? Data control, data security and cost efficiencies over the cloud will be key factors in that decision.

5. Clarification of jurisdiction over the cloud

Clarification of jurisdiction may be read into the ISO/ IEC Standard 27018 rather than expressly stated. For example, to the long-standing questions as to what law applies to the cloud, the Standard specifies that:

- Domestic law determines whether the law applicable to the cloud customer extends to the cloud provider or applies to the cloud customer only;
- The cloud provider must undertake by contract to support and manage domestic privacy law compliance by the cloud customer; and
- In the event of a breach, the cloud provider must share with the cloud customer all the information necessary for the cloud customer to fulfill its legal obligations.

In Canada, these provisions must be read in light of the Accountability Principle whereby the original data holder, in this case the cloud customer, remains responsible for the personal information it collects even when transferred to a data processor, in this case, a cloud provider, and must ensure, in that transfer, a comparable level of protection. Since Canadian privacy law does not offer any more specific guidance in that respect, the provisions of ISO/IEC 27018, delineating respective obligations between the cloud customer and the cloud provider, may be seen as clarifying the legal obligations at hand.

Conclusion: Canada's investment in ISO/IEC27018 and next steps

As I mentioned at the outset, Canada, particularly through the Office of the Privacy Commissioner, has played a leadership role in the development of ISO/IEC Standard 27018. It seems to follow that the next steps would be to foster its implementation in Canada. The following specific measures from federal, provincial and territorial governments, would flow logically from our investment so far:

- Extend directives on privacy protection in relation to third party providers to include model clauses based on ISO/IEC Standard 27018;
- Where data residency requirements exist, remove or relax them to focus on highest data protection, which may in fact be on an ISO/IEC 27018 certified cloud provider, outside Canada; and
- Require use of ISO/IEC certified cloud service providers to ensure the highest level of protection of personal data from Canada in the cloud.

III Comparative Chart

1. Federal Legislation

1.1 Private Sector Privacy Legislation

Canada's private sector privacy legislation is comprised of the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and provincial privacy legislation, including British Columbia's *Personal Information Protection Act*, Alberta's *Personal Information Protection Act,* and Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector.* The provincial statutes have been deemed "substantially similar" to PIPEDA, meaning that the they provide privacy protection that is consistent with and equivalent to that found under PIPEDA; incorporate the privacy principles in PIPEDA; provide for an independent and effective oversight and redress mechanism; and restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate.

Under private sector privacy legislation, an organization is responsible for personal information under its control, including information that has been transferred to a third party for processing. The organization must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

In the Office of the Privacy Commissioner's opinion, the transfer of data to third parties providing cloud computing services is considered a transfer for processing. As a result, organizations that transfer personal information to PII Processors remain accountable for the information and must ensure that the data is properly protected. While private sector privacy legislation may not directly apply to PII Processors, the processors will need to comply with applicable privacy obligations through their contractual relationships with their clients who, as PII Controllers, must ensure that the PII Processors comply with the Act.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5

Private Sector Privacy Principles (Based on PIPEDA Schedule 1)	ISO 27018 Standards
Privacy Obligations Applicable to PII Processors	**Standards that Enable PII Processors to Comply with their Legal Obligations**
Designated Individual: An organization shall designate an individual or individuals who are accountable for the organization's compliance with privacy principles. (4.1.1)	**6.1 Organization of Information Security:** The public cloud PII processor should designate a point of contact for use by the cloud service customer regarding the processing of PII under the contract.
Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. Individuals	**ISO 27018 Global:** The Code of Practice is designed to ensure transparency and provide PII controllers with information about the PII processor's policies and practices.

Private Sector Privacy Principles (Based on PIPEDA Schedule 1)	ISO 27018 Standards
shall be able to acquire information about an organization's policies and practices. (*Note: While this principle is not directly applicable to PII Processors, best practice to ensure transparency generally*). (4.8)	
Privacy Obligations Applicable to PII Controllers	**Standards that Enable PII Processors to Support PII Controller Compliance with their Legal Obligations**
Accountability: An organization is responsible for personal information under its control, including information that has been transferred to a third-party for processing. The organization shall use contractual or other means to provide a comparable level of protection while personal information under its control is being processed by a third-party. (4.1.3)	**5.1 Information Security Policies** • Information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients. • Contractual agreements should clearly allocate responsibility between the PII processor, its sub-contractors and the cloud service customer. • A mechanism to ensure the PII processor is obliged to support and manage compliance is provided by the contract between the cloud service customer and the PII processor.
Identifying Purpose: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. (4.2) • Organization should inform customers that their information may be processed by a third-party service provider. **Limiting Use/Disclosure:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual. (4.5)	**A.2 Purpose Legitimacy and Specification:** PII to be processed under contract should not be processed for any purpose independent of the instructions of the cloud service provider. **A.10.11 Contract Measures:** Contracts between the cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller. **A.2.2 Public Cloud PII Processor's Commercial Use:** PII processed under a contract should not be used by the public PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service. **A.5.1 Use, Retention and Disclosure Limitation:**

Private Sector Privacy Principles (Based on PIPEDA Schedule 1)	ISO 27018 Standards
	The PII processors should provide contractual guarantees that it will reject any requests for PII disclosure that are not legally binding and consult the customer where legally permissible before making any PII disclosure. **A.11 Geographical Location of PII:** The PII processor should specify and document the countries in which PII might possibly be stored (including sub-contracted PII processing).
Limiting Retention: Personal information shall be retained only as long as necessary for the fulfilment of the purposes for which personal information is collected. (4.5) **Destruction:** Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. (4.5.3)	**A.9.3 PII Return, Transfer and Disposal:** The PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer. **A.4 Data Minimization:** Temporary files and documents should be erased or destroyed within a specified, documented period.
Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. (4.7) • Security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. • The methods of protection should include: (i) physical measures (access); (ii) organizational measures (security clearance); and (iii) technological measures (encryption)	**A.10 Information Security Controls (non-exhaustive)** • Confidentiality and NDAs • Protect data on storage media leaving premises • Use of encrypted portable storage media and devices • Encryption of PII transmitted over public-data transmission networks • Implement contracts with sub-contractors that process PII that specify technical and organizational measures to protect PII. **A.9.1 Notification of Data Breach:** PII processor should promptly notify relevant cloud service customer in the event of any unauthorized access to PII or access to processing equipment resulting in loss, disclosure or alteration of PII. Provisions covering the notification should form part of the contract with the customer. **Applicable ISO 27002 Controls:** • **7. Human Resource Security**

Private Sector Privacy Principles (Based on PIPEDA Schedule 1)	ISO 27018 Standards
	• **9. Access Control** • **10. Cryptography:** implement cryptographic control and inform customer of capabilities. • **11. Physical Environmental Security** • **12. Operations Security**: information backup, protection from malware, and logging and monitoring. • **13. Communications Security**: information transfer policies and procedures • **16. Information Security Incident Management**
Individual Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. (4.9) **Accuracy:** Personal information shall be as accurate, complete and up to date as is necessary for the purposes for which it is to be used. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. (4.9)	**A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.

Analysis: ISO 27018 provides a comprehensive framework for the use, disclosure, and protection of PII by PII Processors that meets and exceeds the privacy principles established by Canada's private sector privacy legislation. ISO 27018 requires PII processors to provide customers with customizable solutions that fit the privacy needs of each respective customer, instead of 'take it or leave it' contracts where the PII processors set the parameters of the relationship, often to the detriment of the client's privacy obligations.

1.2 Public Sector Privacy Legislation

Public sector privacy legislation applies to government institutions and the public sector. The statutes set out the privacy rights of Canadians in their interactions with the government. Public sector privacy legislation obligates government institutions to respect the privacy of individuals by controlling the collection, use, disclosure, retention and disposal of personal information. Unlike private sector privacy legislation, provincial public sector legislation applies in a number of instances specifically to PII Processors (i.e. service providers of public bodies). The processors will also have to comply with applicable privacy obligations through their contractual relationships with public bodies.

Privacy Act, RSC, 1985, c P-21 (Federal)

Privacy Act Privacy Principles	ISO 27018 Standards
Privacy Obligations Applicable to federal government institutions (PII Controllers)	**Standards that Enable PII Processors to Support PII Controller Compliance with their Legal Obligations**
Use of Personal Information: Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose. (s 7) **Disclosure of Personal Information:** Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with prescribed exceptions. (s 8)	**A.2 Purpose Legitimacy and Specification:** PII to be processed under contract should not be processed for any purpose independent of the instructions of the cloud service provider. **A.10.11 Contract Measures:** Contracts between the cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller. **A2.2 Public Cloud PII Processor's Commercial Use:** PII processed under a contract should not be used by the PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.
Retention: Personal information that has been used by a government institution for an administrative purpose shall be retained by the institution for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information. (s 6) **Disposal:** A government institution shall dispose of personal information under the control of the institution in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister in relation to the disposal of that information. (s 6)	**A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them. **A.9.3 PII Return, Transfer and Disposal:** The PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer. **A.4 Data Minimization:** Temporary files and documents should be erased or destroyed within a specified, documented period.

Privacy Act Privacy Principles	ISO 27018 Standards
Privacy Obligations Applicable to federal government institutions (PII Controllers)	**Standards that Enable PII Processors to Support PII Controller Compliance with their Legal Obligations**
Individual Access: Every individual who is a Canadian citizen or a permanent resident has a right to and shall, on request, be given access to any personal information about the individual contained in a personal information bank and any other personal information about the individual under the control of a government institution. (s 12) Where an individual is to be given access to personal information requested, the government institution shall permit the individual to examine the information in accordance with the regulation or provide the individual with a copy thereof. (s 17)	**A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.

2. Provincial Legislation

2.1 British Columbia

Freedom of Information and Protection of Privacy Act RSBC 1996 c 165 (British Columbia)

FOIPPA Privacy Principles	ISO 27018 Standards
Privacy Obligations Applicable to Service Providers (PII Processors)	**Standards that Enable PII Processors to Comply with their Legal Obligations**
Unauthorized Disclosure: An employee or associate of a *service provider* who has access, whether authorized or unauthorized, to personal information in the custody or control of a public body, must not disclose that information except as authorized by the Act. (s 30.4) ***'Service provider'*** means a person retained under a contract to perform services for a public body.	**A.5.2 Recording of PII Disclosures:** Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time. **A.11.2 Intended Destination of PII:** PII transmitted using data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.

FOIPPA Privacy Principles	ISO 27018 Standards
Notification of Unauthorized Disclosure: An employee or associate of a *service provider*, who knows that there has been an unauthorized disclosure of personal information that is in the custody or under the control of the public body must immediately notify the head of the public body. (s 30.5)	**A.9.1 Notification of Data Breach:** PII processor should promptly notify relevant cloud service customer in the event of any unauthorized access to PII or access to processing equipment resulting in loss, disclosure or alteration of PII. Provisions covering the notification should form part of the contract with the customer.
Report Foreign Demand for Disclosure: If an employee or associate of a service provider receives a foreign demand for disclosure or has reason to suspect that the unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure, the person must immediately notify the minister responsible for the Act. The notice must include (a) the nature of the foreign demand; (b) who made the demand; (c) when the demand was received; and (d) what information was sought or disclosed in response to the demand. (s 30.2)	**A.5.1 PII Disclosure Notification:** The contract between the PII processor and the cloud service customer should require the PII processor to notify the customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such disclosure is otherwise prohibited. The PII processor should provide contractual guarantees that it will consult the customer where legally permissible before making any PII disclosure.
Privacy Obligations Applicable to Public Bodies (PII Controllers)	**Standards that Enable PII Processors to Support PII Controller Compliance with their Legal Obligations**
Use of Personal Information: A public body may use personal information in its custody or under its control only for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose or if the individual has consented to the use. (s 32) **Disclosure of Personal Information:** A public body may disclose personal information in its custody or under its control *inside or outside of Canada* only with consent, for the purpose for which it was obtained or compiled or for a use consistent with that purpose, or as otherwise permitted by the Act. (s 33)	**A.2 Purpose Legitimacy and Specification:** PII to be processed under contract should not be processed for any purpose independent of the instructions of the cloud service provider. **A.10.11 Contract Measures:** Contracts between cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller. **A2.2 Public Cloud PII Processor's Commercial Use:** PII processed under a contract should not be used by the PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.

FOIPPA Privacy Principles	ISO 27018 Standards
Protection of Personal Information: A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use disclosure or disposal. (s 30)	**A.10 Information Security Controls (non-exhaustive)** • Confidentiality and NDAs • Protect data on storage media leaving premises • Use of encrypted portable storage media and devices • Encryption of PII transmitted over public-data transmission networks • Implement contracts with sub-contractors that process PII that specify technical and organizational measures to protect PII. **A.9.1 Notification of Data Breach:** PII processor should promptly notify relevant cloud service customer in the event of any unauthorized access to PII or access to processing equipment resulting in loss, disclosure or alteration of PII. Provisions covering the notification should form part of the contract with the customer. **Applicable ISO 27002 Controls:** • **7. Human Resource Security** • **9. Access Control** • **10. Cryptography:** implement cryptographic control and inform customer of capabilities. • **11. Physical Environmental Security** • **12. Operations Security:** information backup, protection from malware, and logging and monitoring. • **13. Communications Security:** information transfer policies and procedures • **16. Information Security Incident Management**
Storage and Access Must be in Canada: A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless the individual has consented to it being stored in or accessed from another jurisdiction or if it is stored in or accessed from another jurisdiction as permitted under the Act. (s 30.1)	**A.11 Geographical Location of PII:** The PII processor should specify and document the countries in which PII might possibly be stored (including sub-contracted PII processing).

FOIPPA Privacy Principles	ISO 27018 Standards
Access: An individual has a right of access to any record in the custody or under the control of a public body that contains their personal information. **Retention:** If an individual's personal information is in the custody or under the control of a public body, and is used by or on behalf of the public body to make a decision that directly affects the individual, the public body must ensure that the personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information. (s 31) **Accuracy and Right of Correction:** A public body must make every reasonable effort to ensure that the personal information is accurate and complete. An applicant who believes that there is an error or omission in his or her personal information may request the head of the public body that has the information in its custody or under its control to correct the information. (s 28)	**A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them. **A.9.3 PII Return, Transfer and Disposal:** The PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.

2.2 Nova Scotia

Freedom of Information and Protection of Privacy Act, c 5 of the Acts of 1993/ Personal Information International Disclosure Protection Act, c 3 of the Acts of 2006 (Nova Scotia)

FOIPPA/PIIDPA Privacy Principles	ISO 27018 Standards
Privacy Obligations Applicable to Service Providers (PII Processors)	**Standards that Enable PII Processors to Comply with their Legal Obligations**
Prohibition on Disclosure: A *service provider* who has access, whether authorized or unauthorized, to personal information in the custody or under the control of a public body, shall not disclose that information except as authorized pursuant to the Act. (PIIDPA s 8) ***'Service provider'*** means a person who is retained under a contract to perform services for a public	**A.5.2 Recording of PII Disclosures:** Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time. **A.11.2 Intended Destination of PII:** PII transmitted using data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.

FOIPPA/PIIDPA Privacy Principles	ISO 27018 Standards
body and in the course of performance of the services, uses, discloses, manages, stores or accesses personal information in the custody or under the control of a public body.	
Information to be Stored and Accessed in Canada: 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 the individual who the information is about has consented or has otherwise permitted by the Act. (PIIDPA s 5.1) **Disclosure Outside of Canada:** A service provider shall ensure that personal information in its custody or under its control is disclosed outside Canada only in accordance with the Act. (PIIDPA s 9)	**A.11 Geographical Location of PII:** The PII processor should specify and document the countries in which PII might possibly be stored (including sub-contracted PII processing). **A.5.2 Recording of PII Disclosures:** Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time. **A.11.2 Intended Destination of PII:** PII transmitted using data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.
Storage, Access and Disclosure Outside of Canada: In providing storage, access or disclosure of personal information outside of Canada, a service provider 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. (PIIDPA s 5(4))	**A.10 Information Security Controls (non-exhaustive)** • Confidentiality and NDAs • Protect data on storage media leaving premises • Use of encrypted portable storage media and devices • Encryption of PII transmitted over public-data transmission networks • Implement contracts with sub-contractors that process PII that specify technical and organizational measures to protect PII. **Applicable ISO 27002 Controls:** • **7. Human Resource Security** • **9. Access Control** • **10. Cryptography:** implement cryptographic control and inform customer of capabilities. • **11. Physical Environmental Security** • **12. Operations Security:** information backup, protection from malware, and logging and monitoring. • **13. Communications Security:** information transfer policies and procedures

FOIPPA/PIIDPA Privacy Principles	ISO 27018 Standards
	• **16. Information Security Incident Management**
Foreign Demand for Disclosure: where a service provider receives a foreign demand for disclosure, receives a request to disclose or has reason to suspect that unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure, the service provider shall immediately notify the Minister. The notice must include the nature of the foreign demand, who made the foreign demand; when the foreign demand was received; and what information was sought. (PIIDPA s 6)	**A.5.1 PII Disclosure Notification:** The contract between the PII processor and the cloud service customer should require the PII processor to notify the customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such disclosure is otherwise prohibited. The PII processor should provide contractual guarantees that it will consult the customer where legally permissible before making any PII disclosure.
Privacy Obligations Applicable to Public Bodies (PII Controllers)	**Standards that Enable PII Processors to Support PII Controller Compliance with their Legal Obligations**
Use of Personal Information: A public body may use personal information only for the purpose for which that information was obtained or compiled, or for use compatible with that purpose, or if the individual the information is about has consented to the use, or as otherwise permitted by the Act. (FOIPPA s 26) **Disclosure of Personal Information:** A public body may disclose personal information only with consent, for the purpose for which it was obtained or compiled or for a use consistent with that purpose, or as otherwise permitted by the Act. (FOIPPA s 27)	**A.2 Purpose Legitimacy and Specification:** PII to be processed under contract should not be processed for any purpose independent of the instructions of the cloud service provider. **A.10.11 Contract Measures:** Contracts between cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller. **A2.2 Public Cloud PII Processor's Commercial Use:** PII processed under a contract should not be used by the PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.
Protection of Personal Information: The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. (FOIPPA s 24(3))	**A.10 Information Security Controls (non-exhaustive)** • Confidentiality and NDAs • Protect data on storage media leaving premises • Use of encrypted portable storage media and devices • Encryption of PII transmitted over public-data transmission networks

FOIPPA/PIIDPA Privacy Principles	ISO 27018 Standards
	• Implement contracts with sub-contractors that process PII that specify technical and organizational measures to protect PII. **A.9.1 Notification of Data Breach:** PII processor should promptly notify relevant cloud service customer in the event of any unauthorized access to PII or access to processing equipment resulting in loss, disclosure or alteration of PII. Provisions covering the notification should form part of the contract with the customer. **Applicable ISO 27002 Controls:** • **7. Human Resource Security** • **9. Access Control** • **10. Cryptography:** implement cryptographic control and inform customer of capabilities. • **11. Physical Environmental Security** • **12. Operations Security:** information backup, protection from malware, and logging and monitoring. • **13. Communications Security:** information transfer policies and procedures • **16. Information Security Incident Management**
Information to be Stored and Accessed in Canada: A public body shall ensure that personal information in its custody or under its control is stored only in Canada, unless the individual who the information is about has consented or as otherwise permitted by the Act. (PIIDPA s 5) **Disclosure Outside Canada:** A public body shall ensure that personal information in its custody or under its control is disclosed outside Canada only in accordance with the Act. (PIIDPA s 9)	**A.11 Geographical Location of PII:** The PII processor should specify and document the countries in which PII might possibly be stored (including sub-contracted PII processing). **A.10.11 Contract Measures:** Contracts between cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller.
Access: A person has a right of access to any record in the custody or under the control of a public body (subject to exemptions). The head of a public body must make every reasonable effort to assist the applicant and to respond without delay. (FOIPPA s 5)	**A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.

FOIPPA/PIIDPA Privacy Principles	ISO 27018 Standards
Retention: Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body shall retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it. (FOIPPA s 24(4)) **Accuracy and Right of Correction:** An applicant who believes there is an error or omission in the applicant's personal information may request the head of the public body that has the information in its custody or under its control to correct the information. Upon being notified of a correction of personal information, a public body shall make the correction on any record of that information in its custody or under its control. (FOIPPA s 25)	**A.9.3 PII Return, Transfer and Disposal:** The PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.

2.3 Quebec

An Act respecting Access to Documents held by Public Bodies and the Protection of Personal Information (Quebec) P39.1

Quebec Public Sector Privacy Principles	ISO 27018 Standards
Privacy Obligations Applicable to Public Bodies (PII Controllers)	**Standards that Enable PII Processors to Support PII Controller Compliance with their Legal Obligations**
Use of Personal Information: Personal information may not be used within a public body except for the purposes for which it was collected. A public body may, however, use such information for another purpose with consent or without consent, but only if the information is used for purposes consistent with the purposes for which it was collected or as otherwise permitted by the Act. (s 65.1) **Disclosure of Personal Information:** A public body must obtain consent to release personal information unless as otherwise permitted by the Act. Where a public body releases personal information pursuant to such exemptions, the public body must record in a register every such release	**A.2 Purpose Legitimacy and Specification:** PII to be processed under contract should not be processed for any purpose independent of the instructions of the cloud service provider. **A.10.11 Contract Measures:** Contracts between cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller. **A2.2 Public Cloud PII Processor's Commercial Use:** PII processed under a contract should not be used by the PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving

Quebec Public Sector Privacy Principles	ISO 27018 Standards
of personal information. (s 59)	the service.
Security Measures: A public body must take the security measures necessary to ensure the protection of the personal information collected, used, released, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored. (s 63.1)	**A.10 Information Security Controls (non-exhaustive)** • Confidentiality and NDAs • Protect data on storage media leaving premises • Use of encrypted portable storage media and devices • Encryption of PII transmitted over public-data transmission networks • Implement contracts with sub-contractors that process PII that specify technical and organizational measures to protect PII. **A.9.1 Notification of Data Breach:** PII processor should promptly notify relevant cloud service customer in the event of any unauthorized access to PII or access to processing equipment resulting in loss, disclosure or alteration of PII. Provisions covering the notification should form part of the contract with the customer. **Applicable ISO 27002 Controls:** • **7. Human Resource Security** • **9. Access Control** • **10. Cryptography:** implement cryptographic control and inform customer of capabilities. • **11. Physical Environmental Security** • **12. Operations Security:** information backup, protection from malware, and logging and monitoring. • **13. Communications Security:** information transfer policies and procedures • **16. Information Security Incident Management**
Release of Information Outside of Quebec: Before releasing personal information outside Quebec or entrusting a person or a body outside Quebec with the task of holding, using or releasing	**A.11 Geographical Location of PII:** The PII processor should specify and document the countries in which PII might possibly be stored

Quebec Public Sector Privacy Principles	ISO 27018 Standards
such information on its behalf, a public body must ensure that the information receives protection equivalent to that afforded under this Act. (s 70.1)	(including sub-contracted PII processing). **A.10.11 Contract Measures:** Contracts between cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller. **A.2 Purpose Legitimacy and Specification:** PII to be processed under contract should not be processed for any purpose independent of the instructions of the cloud service provider. **A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.
Access: Every person has the right to be informed of the existence of personal information concerning him in a personal information file and a right to obtain any personal information kept on him (subject to the Act). (s 83) **Right of Correction:** Every person who receives confirmation of the existence of personal information concerning him may request that the file be corrected if the information is inaccurate, incomplete or equivocal or if the collection, release or keeping of the information is not authorized by law. (s 89)	**A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them. **A.9.3 PII Return, Transfer and Disposal:** The PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.

2.4 Alberta

Freedom of Information and Protection of Privacy Act (Alberta) RSA 2000, Chapter F-25

FOIPPA Privacy Principles	ISO 27018 Standards
Privacy Obligations Applicable to Public Bodies (PII Controllers)	**Standards that Enable PII Processors to Support PII Controller Compliance with their Legal**

FOIPPA Privacy Principles	ISO 27018 Standards
	Obligations
Use of Personal Information: A public body may use personal information only for the purposes for which the information was collected or compiled or for a use consistent with that purpose or if the individual identified has consented to the use or as otherwise permitted by the Act. (s 39(1)) **Disclosure of Personal Information:** A public body may disclose personal information only for the purposes for which the information was collected or compiled or for a use consistent with that purpose or if the individual identified has consented to the disclosure, or as otherwise permitted by the Act. (s 40(1))	**A.2 Purpose Legitimacy and Specification:** PII to be processed under contract should not be processed for any purpose independent of the instructions of the cloud service provider. **A.10.11 Contract Measures:** Contracts between cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller. **A2.2 Public Cloud PII Processor's Commercial Use:** PII processed under a contract should not be used by the PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service. **A.11 Geographical Location of PII:** The PII processor should specify and document the countries in which PII might possibly be stored (including sub-contracted PII processing).
Protection of Personal Information: The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction. (s 38)	**A.10 Information Security Controls (non-exhaustive)** • Confidentiality and NDAs • Protect data on storage media leaving premises • Use of encrypted portable storage media and devices • Encryption of PII transmitted over public-data transmission networks • Implement contracts with sub-contractors that process PII that specify technical and organizational measures to protect PII. **A.9.1 Notification of Data Breach:** PII processor should promptly notify relevant cloud service customer in the event of any unauthorized access to PII or access to processing equipment resulting in loss, disclosure or alteration of PII. Provisions covering the notification should form part of the contract with the customer. **Applicable ISO 27002 Controls:**

FOIPPA Privacy Principles	ISO 27018 Standards
	• **7. Human Resource Security** • **9. Access Control** • **10. Cryptography:** implement cryptographic control and inform customer of capabilities. • **11. Physical Environmental Security** • **12. Operations Security:** information backup, protection from malware, and logging and monitoring. • **13. Communications Security:** information transfer policies and procedures • **16. Information Security Incident Management**
Access: An individual has a right of access to any record in the custody or under the control of the public body that contains personal information about the applicant. (s 6) **Retention:** If an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body must retain the personal information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it. (s 35) **Accuracy and Right of Correction:** If an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body must make every reasonable effort to ensure that the information is accurate and complete. An individual who believes that there is an error or omission in their personal information may request the head of the public body that has the information in its custody or under its control to correct the information. (s 35)	**A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them. **A.9.3 PII Return, Transfer and Disposal:** The PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.

2.5 Ontario

Freedom of Information and Protection of Privacy Act (Ontario) RSO 1990, Chapter F.31

FOIPPA Privacy Principles	ISO 27018 Standards
Privacy Obligations Applicable to Public Bodies (PII Controllers)	**Standards that Enable PII Processors to Support PII Controller Compliance with their Legal Obligations**
Use of Personal Information: An institution shall not use personal information in its custody or under its control except, (a) where the person to whom the information relates has consented to its use; (b) for the purpose for which it was obtained or compiled or for a consistent purpose; or (c) other prescribed purposes. (s 41) **Disclosure of Personal Information:** An institution shall not disclose personal information in its custody or under its control except in accordance with the Act. (s 42)	**A.2 Purpose Legitimacy and Specification:** PII to be processed under contract should not be processed for any purpose independent of the instructions of the cloud service provider. **A.10.11 Contract Measures:** Contracts between cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller. **A2.2 Public Cloud PII Processor's Commercial Use:** PII processed under a contract should not be used by the PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.
Retention: Personal information that has been used by an institution shall be retained after use by the institution for the period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the personal information. (s 40) **Disposal:** A head shall dispose of personal information under the control of the institution in accordance with the regulations. (s 40(4))	**A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them. **A.9.3 PII Return, Transfer and Disposal:** The PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer. **A.4 Data Minimization:** Temporary files and documents should be erased or destroyed within a specified, documented period.

FOIPPA Privacy Principles	ISO 27018 Standards
Individual Access: Every individual has a right of access to any personal information about the individual in the custody or under the control of an institution. (s 47(1)) **Right of Correction:** Every individual who is given access to personal information is entitled to request correction of the personal information where the individual believes there is an error or omission therein. (s 47(2))	**A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.

Analysis: Unlike private sector privacy legislation, provincial public sector privacy legislation places privacy obligations on PII Processors. Specifically, public sector legislation obligates PII Processors to abide by certain requirements regarding personal information in the custody or under the control of a public body, including the following:

- Prohibition on the unauthorized disclosure of personal information;
- Notification of unauthorized disclosure of personal information;
- Personal information must be stored and accessed in Canada, unless otherwise permitted by legislation;
- Personal information that is disclosed outside of Canada must be done so in accordance with legislation; and
- Reporting of foreign demands for disclosure of personal information.

In addition, PII Processors must help public bodies abide by requirements regarding the disclosure or release of information outside of Canada or a province.

ISO 27018 establishes standards for PII Processors that sufficiently address their obligations under provincial public sector privacy legislation, including with respect to unauthorized disclosure of personal information and the storage, access, and disclosure of personal information abroad. Nevertheless, one minor 'gap' in the legislation is the specificity of the Geographical Location of PII standard requiring PII Processors to specify and document the *countries* in which PII might possibly be stored in order to help both PII Processors and public sector bodies comply with the requirements under provincial legislation. Quebec legislation governs the release of information outside of Quebec, not merely Canada. The Geographical Location of PII standard should more broadly refer to sub-national jurisdictions (e.g. provinces or states), rather than only a country-basis. However, this is a relatively minor issue.

3. Personal Health Information Privacy Legislation

A health information custodian is responsible for personal health information in its custody or control (PII Controller). While a PII Processor is not considered a health information custodian under health information privacy legislation, a processor may be considered a 'provider to a custodian', a 'health information network provider', or an 'agent' under such legislation. These persons are permitted to collect,

use, disclose, retain or dispose of personal health information on the custodian's behalf, but are subject to prescribed requirements, particularly with respect to security of personal health information.

Personal Health Information Protection Act, 2004, Ontario Regulation 329/04

PHIPA Privacy Principles	ISO 27018 Standards
Privacy Obligations Applicable to Service Providers (PII Processors)	**Standards that Enable PII Processors to comply with their Legal Obligations**
Providers to Custodians "*Providers to Custodians"* means a person who provides goods or services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information. **Restriction on Persons who Provide to Custodians:** The following are requirements for persons who provide to custodians who are not agents of the custodian: (s 6 Regulations) • The person shall not use any personal health information to which it has access in the course of providing the services for the custodian except as necessary in the course of providing the services; • The person shall not disclose any personal health information to which it has access; • The person shall not permit its employees or any person acting on its behalf to be able to have access to the information unless the employee or person agrees to comply with the restrictions that apply to the person who provide to custodians.	**A.2 Purpose Legitimacy and Specification:** PII to be processed under contract should not be processed for any purpose independent of the instructions of the cloud service provider. **7. Human Resource Security:** Management is responsible for implementing guidelines to employees. Measures should be put in place to make staff aware of the possible consequences on the PII processor of breaching privacy or security rules and procedures, especially those addressing the handling of PII. **A.10.1 Confidentiality or Non-Disclosure Agreements:** Individuals under the public cloud processor's control with access to PII should be subject to a confidentiality obligation. **A.10.12 Sub-contracted PII Processing:** Contracts between the PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the PII processor.
Health Information Network Providers (Type of Provider) *"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(3) Regulations) **Requirements on Health Information Network**	**A.9.1 Notification of Data Breach:** PII processor should promptly notify relevant cloud service customer in the event of any unauthorized access to PII or access to processing equipment resulting in loss, disclosure or alteration of PII. Provisions covering the notification should form part of the contract with the customer. In the event of a data breach, a record should be maintained with a description of the incident, the time period, the consequences, the name of the report, to whom the incident was reported, the steps taken to resolve the incident and the fact that the incident resulted in

PHIPA Privacy Principles	ISO 27018 Standards
Providers: • The provider shall notify every custodian if the provider accessed, used, disclosed or disposed of personal health information other than in accordance with the Regulations or an unauthorized person accessed the personal health information; • The provider shall provide each custodian with a plain language description of the services that the provider provides to the custodians, including a general description of the safeguards in place to protect against unauthorized use and disclosure and to protect integrity of information. • The provider shall make available to the public any guidelines and policies that it provides to custodians and a general description of the safeguards implemented. • The provider shall, to the extent practical, keep and make available to each custodian, on the request, an electronic record of all access to all or part of the personal health information associated with the custodian being held in equipment controlled by the provider (who, date and time) and all transfers of all or part of the information associated with the custodian by means of equipment controlled by the provider (who, date and time). • The provider shall perform and provide to each custodian a copy of the results of an assessment of the services provided to the custodians with respect to threats, vulnerabilities and risks to the security and integrity of the health information and how the services may affect the privacy of individuals who are the subject of the information. • The provider shall ensure that any third party it retains to assist in providing services agrees to comply with the restrictions and conditions that are necessary to enable the provider to comply with this section.	loss, disclosure or alteration of PII. **A.5.2 Recording of PII Disclosures:** Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time. **A.10 Information Security (User IDs and Access Records):** If more than one individual has access to stored PII, then they should each have a distinct User ID for identification, authentication and authorization purposes. An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained. **12.4 Logging and Monitoring:** A process should be put in place to review event logs with a specified, documented periodicity, to identify irregularities and propose remediation efforts. Where possible, event logs should record whether or not PII has changed as a result of an event and by whom. The PII processor should define criteria regarding if, when and how log information can be made available to or usable by the cloud service customer. **5.1 Information Security Policies** Information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients. Contractual agreements should clearly allocate responsibility between the PII processor, its sub-contractors and the cloud service customer. A mechanism to ensure the PII processor is obliged to support and manage compliance is provided by the contract between the cloud service customer and the PII processor. **A.10.12 Sub-contracted PII Processing:** Contracts between the PII processor and any sub-contractors that process PII should specify

PHIPA Privacy Principles	ISO 27018 Standards
• The provider shall enter into a written agreement with each custodian concerning the services provided to the custodian that describes the services that the provider is required to provide to the custodian and the administrative, technical and physical safeguards relating to the confidentiality and security of the information.	minimum technical and organizational measures that meet the information security and PII protection obligations of the PII processor. **A.10.11 Contract Measures:** Contracts between cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller.
Agents *"Agent"* means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated. (s 2 Act) **Restriction on Agents:** An *agent* of a health information custodian shall not collect, use, disclose, retain or dispose of personal health information on the custodian's behalf unless the custodian permits the agent to do so in accordance with the Act. **Use of Personal Health Information:** If a health information custodian is authorized to use health information for a permitted purpose (e.g. payment processing), the custodian may provide the information to an agent of the custodian who may use it for that purpose on behalf of the custodian. (s 37(2) Act) **Notification:** An agent of a health information custodian shall notify the custodian at the first reasonable opportunity if personal health information handled by the agent on behalf of the custodian is stolen, lost or accessed by unauthorized persons. (s 17(3) Act)	**A.2 Purpose Legitimacy and Specification:** PII to be processed under contract should not be processed for any purpose independent of the instructions of the cloud service provider. **A.10.11 Contract Measures:** Contracts between cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller. **A.9.1 Notification of Data Breach:** PII processor should promptly notify relevant cloud service customer in the event of any unauthorized access to PII or access to processing equipment resulting in loss, disclosure or alteration of PII. Provisions covering the notification should form part of the contract with the customer.
Privacy Obligations Applicable to Health Information Custodians (PII Controllers)	**Standards that Enable PII Processors to Support PII Controller Compliance with their Legal Obligations**

PHIPA Privacy Principles	ISO 27018 Standards
Use of Personal Health Information: A health information custodian may use personal health information about an individual for the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose, unless the individual expressly instructs otherwise or as otherwise authorized by the Act. (s 37(1) Act) **Use and Disclosure of Personal Health Information:** a health information custodian shall not use or disclose personal health information about an individual unless it has the individual's consent or the use/disclosure is permitted or required by the Act. (s 31 Act) **Marketing:** A health information custodian shall not use or disclose personal health information about an individual for the purpose of marketing anything or for the purpose of market research unless the individual expressly consents and subject to restrictions. (s 33 Act)	**A.2 Purpose Legitimacy and Specification:** PII to be processed under contract should not be processed for any purpose independent of the instructions of the cloud service provider. **A.10.11 Contract Measures:** Contracts between cloud service customer and the PII processor should specify minimal technical and organizational measures to ensure that data is not processed for any purpose independent of the instructions of the controller. **A2.2 Public Cloud PII Processor's Commercial Use:** PII processed under a contract should not be used by the PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.
Disclosure outside Ontario: A health information custodian may disclose personal information about an individual collected in Ontario to a person outside Ontario only if (a) the individual consents to the disclosure; (b) the Act permits the disclosure; (c) the person receiving the information performs functions comparable to the functions performed by a person to whom the Act would permit the custodian to disclose the information in Ontario and other prescribed requirements. (s 50(1) Act)	**A.11 Geographical Location of PII:** The PII processor should specify and document the countries in which PII might possibly be stored (including sub-contracted PII processing).
Security: A healthcare custodian that discloses personal health information about an individual shall take reasonable steps to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. (s 12(1) Act) **Notice of Loss:** A health information custodian that has custody or control of personal health	**A.10 Information Security Controls (non-exhaustive)** • Confidentiality and NDAs • Protect data on storage media leaving premises • Use of encrypted portable storage media and devices • Encryption of PII transmitted over public-data transmission networks • Implement contracts with sub-contractors that process PII that specify technical and organizational measures to protect PII.

PHIPA Privacy Principles	ISO 27018 Standards
information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons. (s 12(2) Act)	**A.9.1 Notification of Data Breach:** PII processor should promptly notify relevant cloud service customer in the event of any unauthorized access to PII or access to processing equipment resulting in loss, disclosure or alteration of PII. Provisions covering the notification should form part of the contract with the customer. **Applicable ISO 27002 Controls:** • **7. Human Resource Security** • **9. Access Control** • **10. Cryptography:** implement cryptographic control and inform customer of capabilities. • **11. Physical Environmental Security** • **12. Operations Security:** information backup, protection from malware, and logging and monitoring. • **13. Communications Security:** information transfer policies and procedures **16. Information Security Incident Management**
Handling of Records: A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with prescribed requirements. (s 13(1) Act)	**A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them. **A.9.3 PII Return, Transfer and Disposal:** The PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer. **A.4 Data Minimization:** Temporary files and documents should be erased or destroyed within a specified, documented period.
Right of Access: An individual has a right of access to a record of personal health information about the individual that is in the custody or under the control of a health information custodian (subject to exceptions). (s 52(1) Act) **Correction:** If a health information custodian has	**A.1 Obligation to Co-operate Regarding PII Principals' Rights:** The PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.

PHIPA Privacy Principles	ISO 27018 Standards
granted an individual access to a record of his or her personal health information and if the individual believes that the record is inaccurate or incomplete for the purposes for which the custodian has collected, uses or has used the information, the individual may request that the custodian correct the record. (s 55 Act)	

Analysis: Similar to provincial public sector privacy legislation, provincial personal health information privacy legislation places privacy obligations on PII Processors. Specifically, the legislation may obligate PII Processors, depending on whether they are characterized as service providers or agents, to abide by certain requirements regarding personal health information, including the following:

- Requirement to enter into a written agreements with health custodians regarding the services to be provided and the practices, policies, and security measures of the PII Processor;
- Prohibition on the use of personal health information in the course of providing services for health custodians except as necessary in the course of providing the service;
- Prohibition on the unauthorized disclosure of personal health information;
- Maintenance of records and logs regarding access to personal health information;
- Notification of unauthorized disclosure of personal health information;
- Restrictions on employee access to personal health information; and
- Perform and provide to custodians an assessment of threats, vulnerabilities, and risks (ongoing basis).

In addition, PII Processors must help health custodians abide by requirements regarding the disclosure of information outside of the applicable province and the prohibition on using personal health information for marketing purposes.

ISO 27018 establishes standards for PII Processors that sufficiently address their obligations under provincial personal health information privacy legislation. However, there are a number of minor 'gaps' that should be acknowledged. First, the Geographical Location of PII standard requiring PII Processors to specify and document the *countries* in which PII might possibly be stored in order to help both PII Processors and health custodians comply with the requirements under provincial legislation is too broad considering that personal health information is governed on a provincial basis and the out-bound disclosure rules apply on a provincial level. Second, ISO 27018 does not explicitly require PII Processors to provide clients with an ongoing report regarding threats, vulnerabilities and risks to their personal health information. This though may be covered under broader standards requiring PII Processors to help PII Controllers comply with privacy legislation.

The foregoing analysis also assumes that PII Processors have a mechanism in place to distinguish between different types of personal information and implement their obligations accordingly.

About Dentons

Dentons is a global firm driven to provide a competitive edge in an increasingly complex and interconnected marketplace. It was formed in March 2013 by the combination of international law firm Salans LLP, Canadian law firm Fraser Milner Casgrain LLP (FMC) and international law firm SNR Denton. Dentons is built on the solid foundations of these three highly valued law firms. Each built an outstanding reputation and valued clientele by responding to the local, regional and national needs of a broad spectrum of clients of all sizes – individuals; entrepreneurs; small businesses and start-ups; local, regional and national governments and government agencies; and mid-sized and larger private and public corporations, including international and global entities.

Dentons' clients now benefit from approximately 6,600 lawyers and professionals in more than 75 locations spanning 50-plus countries across Africa, Asia Pacific, Canada, Central Asia, Europe, the Middle East, Russia and the CIS, the UK and the US who are committed to challenge the status quo and offer creative, dynamic business and legal solutions.

Chantal Bernier
Dentons Canada LLP
1420-99 Bank Street
Ottawa, ON K1P 1H4

Chantal.Bernier@Dentons.com
D +1 613 783 9684
T +1 613 783 9600
F +1 613 783 9690

© 2015 Dentons. This document is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. We are providing information to you on the basis you agree to keep it confidential. If you give us confidential information but do not instruct or retain us, we may act for another client on any matter to which that confidential information may be relevant. Attorney Advertising. Please see dentons.com for Legal Notices.

Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. [Insert Location Text]