Solutions for Healthcare

Providing secure, Canadian resident, Infrasturcture-as-a-Service for Healthcare Technology Solutions

Cloud-A's Guide to Protecting Private Healthcare Information in the Canadian Public Cloud

We have been receiving a lot of questions from prospective partners about how we comply with the rules around private information as it pertains to healthcare in Canada. The simple answer is that we provide secure and redundant infrastructure to our healthcare partners and work with them to recommend best practices and procedures for securing their own virtual instances that reside on our public cloud.

While that explanation might seem broad for such an important topic, the laws pertaining to personal information protection in Canada are complicated, technically nonspecific, and just plain hard to grasp.

Information Privacy in Canadian Healthcare

The Canadian law relating to data privacy is called the Personal Information Protection and Electronic Documents Act (PIPEDA). According to the Canadian government, the goal of this law is to set out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. PIPEDA applies to all commercial activities by organizations in all provinces, except for six provinces who have their own version of the law (British Columbia, Alberta, Ontario, Quebec, Newfoundland & Labrador, and New Brunswick).

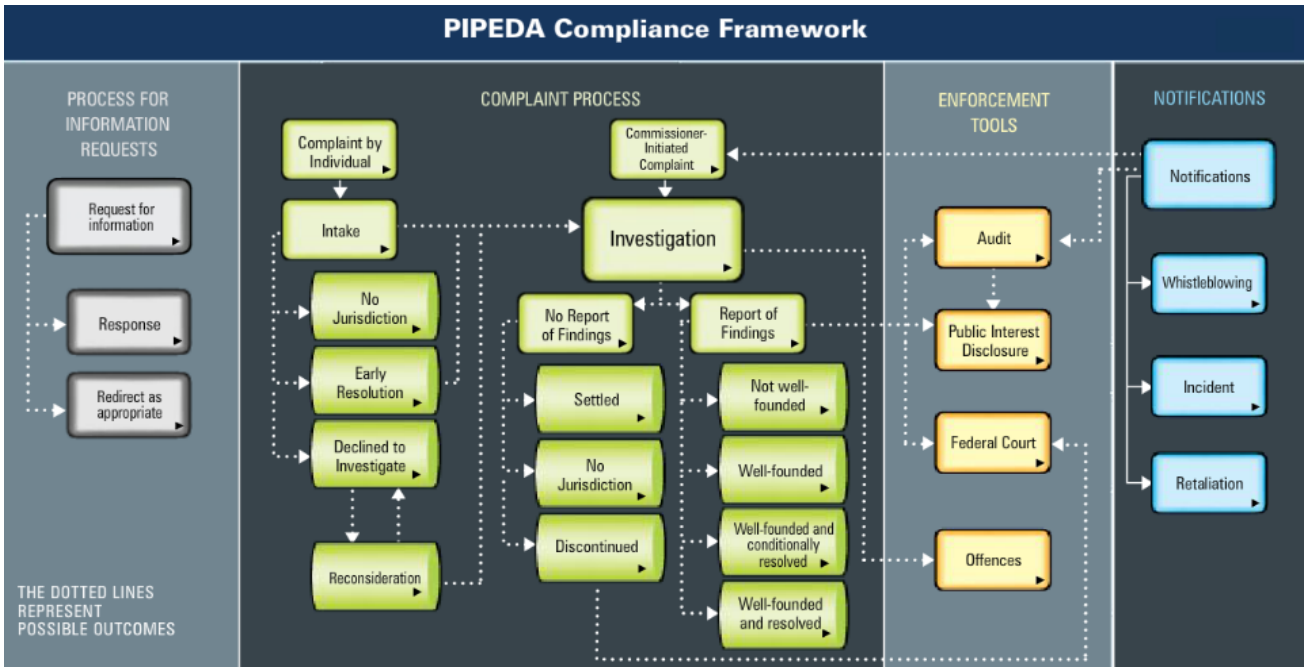
PIPEDA requires organizations to take reasonable steps to safeguard the personal information that they manage from risks that the government defines as: unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

Some safeguards that the government deems reasonable include but are not limited to:

- risk management
- security policies
- human resources security
- physical security
- technical security
- incident management
- business continuity planning

The reasonableness of security arrangements adopted by an organization must be evaluated in light of a number of factors including:

- the sensitivity of the personal information
- the foreseeable risks
- the likelihood of damage occurring
- the medium and format of the record containing the personal information
- the potential harm that could be caused by an incident
- the cost of preventive measures



https://www.priv.gc.ca/leg_c/frame/pipeda_cf_e.swf

PIPEDA in the Cloud

Cloud computing is not prohibited by PIPEDA. In fact, the same rules that apply to storing private information on locally run infrastructure would apply if the same information was stored on Cloud-A's Infrastructure-as-a-service. Organizations must ensure that they collect personal information for appropriate purposes and that these purposes be made clear to individuals; they obtain consent; they limit collection of personal information to those purposes; they protect the information; and that they be transparent about their privacy practices.

One important thing to consider when using any cloud product with personal information is that the organization who transfers the personal information to the 3rd party (cloud provider) remains accountable for that data. It is the responsibility of the data transferring organization to perform due diligence to ensure that they are comfortable with the security and redundancy of the cloud provider's platform. This process in itself becomes a partnership between the data transferring organization and the cloud provider.

Partnering with Cloud-A for Private Data Security

Cloud-A prides ourself on enabling our partners to offer high performing, highly secure, Canadian resident solutions. In addition to maintaining bulletproof infrastructure, we work closely with our partners and provide them with the tools to ensure that their cloud infrastructure is secure.

Canadian Data Residency

Our Commitment:

All Cloud-A physical infrastructure, systems, offices, employees and ownership are in Canada. Always. No client data will ever be moved without notification.

Partner Responsibility:

To ensure that client data is always resident in Canada, it is the partner's responsibility to ensure that their data is organized and accounted for within their Cloud-A infrastructure. It is important to be aware of multiple copies of data that you may have previously stored on another non-Canadian cloud provider's infrastructure.

Security

Our Commitment:

- Cloud-A operates in a TIA 942 Tier III data centre which is equipped with complete physical security: perimeter alarms, biometric authentication, CCTV monitoring and historical 30+ day records.
- Cloud-A provides our partners with all of the tools to setup secure networks with our virtual private networking.
- All client networks are fully encrypted and segregated.
- All virtual servers are individually contained and segregated with both a hypervisor and AppArmor which limits the data access ability of a VM to only that VM's specific data.

Partner Responsibility:

Partners are responsible for using unique, secure passwords on their instances, encrypting their drives, creating and managing secure virtual private networks, performing updates and patching as required, and monitoring and auditing their instances.

Redundancy

Our Commitment:

- Cloud-A only operates redundant, enterprise class infrastructure (storage, servers and networking) and software capable of live migration and automatic failover within the data centre
- Cloud-A's Data centre has multiple upstream data and internet connections to Tier 1 carriers and providers, 2N In-line UPS system, high-capacity Uninterruptible Power Supplies, 3 phase 120-208 V K-13 PDUs, state-of-the-art fire suppression systems, and multiple backup diesel generators with extended on-site fuel storage (72 hours+)

Partner Responsibility:

Cloud-A partners are responsible for properly backing up the data that resides on their virtual infrastructure.

Summary

It is no secret that the laws protecting personal private information in Canada are confusing, so it is no wonder that we have partners who come to us for guidance on how to be compliant when managing this type of data in the public cloud. Cloud-A is committed to providing our healthcare partners with the secure, redundant, Canadian resident infrastructure they need to feel comfortable handling personal information, and we are more than happy to provide documentation and resources to assist with partners' PIPEDA compliance requirements.

Resources

Personal Information Protection and Electronic Documents Act

British Columbia's *Personal Information Protection Act*
Alberta's *Personal Information Protection Act*
Québec's An Act Respecting the Protection of Personal Information in the Private Sector
Ontario's *Personal Health Information Protection Act*
New Brunswick's *Personal Health Information Privacy and Access Act*
Newfoundland and *Labrador's Personal Health Information Act*

Securing Personal Information: A Self-Assessment Tool for Organizations

Office of the Privacy Commissioner of Canada: Introduction to Cloud Computing

---