TECHNATION CA

Questions and Answers on Privacy & Security Framework

Cyber Security

Cyber Security Question: What are some of the challenges that health organizations face in dealing with threats by bad actors in cyber security?

Personal identifiable health information is considered the most sensitive information about individuals. Health organization are challenged to respond to increasing sophisticated attacks to its information systems and personal health information in its custody and control. Without a practical approach to implement an effective cybersecurity program, this will lead to unauthorized access of a patient's health information. Ransomware attacks on a health organization may result in significant disruption of health services and incur significant legal and financial liabilities.

Cyber Security Question: What are some constructive strategies can small and medium sized enterprises (SMEs) embrace to reduce risk of cyber security incidents?

SMEs should adopt an internationally recognized security standard to protect personal health information. While the cost of implementing a typical international security standard such as the ISO/IEC 27001 is very expensive, there is another practical alternative available for Canadian SMEs. The Canadian Centre for Cyber Security has developed knowledge content and education materials specifically with SMEs in mind. This includes Cybersecure, a certification program sponsored by the Government of Canada.

CyberNB is providing enabling support for community participation. The shared services include cyber security controls that extend across the participating organizations.

Ontario's Centennial College Online cybersecurity governance courses offers certification and provides cybersecurity standards not only for Canada, US & Europe. They have already provided courses for different SMEs & enterprises from different regions in Canada, US & Europe. After having taken their online cybersecurity governance courses, these organizations have been able to save on their cybersecurity insurance as well. They have partnered with HIMSS (where organizations who exercise this training also get HIMSS CE credits) & New York Academy of Sciences.

CIS CONTROLS allow for smaller organizations to focus on the top items that give them the most bang for their buck.

https://www.cisecurity.org/controls/cis-controls-list/

The CIS Center for Internet Security have identified the top 20 security controls, but they break it down nicely into

- *6 basic controls*
- *10 foundational controls*
- *4 organizational controls*

Cyber Security Question: With recent emergence of artificial intelligence in counteracting cyber security threats, who is leading on AI technology use in Canadian health organizations? Has the AI technology been considered from an ethical perspective? Is there a third party that will continuously monitor the AI technology? If so, who will be held responsible for this task and who will they report to?

AI is an umbrella term that includes a range of technologies — including machine learning, computer vision, natural language processing, deep learning, etc. These technologies are in various stages of new development and deployment. There are several AI applications being deployed by enterprise organizations to assist in automating and hardening their cyber security protection. Very interesting work is in progress in Canada on integration of AI with IoT and IoMT (medical equipment) to protect these devices from cyber threats.

Data Sovereignty

Data Sovereignty Question: Why is consistent data sovereignty policy important for HIT vendors?

Data Sovereignty refers to geopolitical restrictions on the access, storage, and/or use of data. Inconsistent rules within and across jurisdictions cause considerable confusion in the marketplace. Having consistent policy across all of the Canadian jurisdictions means that HIT vendors can provide, especially cloud-based services, solutions that are common, rather than needing to be customized for each jurisdictions.

Data Sovereignty Question: Does Canada and its vendor community have sufficient data centre capacity to support the expanding health cloud services?

In Canada, Data sovereignty restrictions were implemented in three provinces in response to the US Patriot Act following the 9/11 attacks in 2001. The Patriot Act, and its successor legislation, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) give US authorities access to certain data extraterritorially. British Columbia's Freedom of Information and Protection of Privacy Act, Nova Scotia's Personal Information International Disclosure Protection Act, and New Brunswick's Personal Health Information Privacy and Access Act require that personal information be accessed from, or stored in Canada, subject to narrowly defined exemptions.

In response to data sovereignty restrictions, many Cloud providers have established data centers in Canada capable of enabling data sovereignty on a national level. This includes Amazon Web Services, Microsoft Azure, Google Cloud, and IBM Cloud. Significant investments have already been made by these companies for data centres and infrastructure within Canada's borders to enable Cloud and shared service platforms.

Data Sovereignty Question: If all Canadian jurisdictions adopted standardized rules for data sovereignty, what positive outcomes could be realized?

Standardization of data sovereignty would enable more rapid adoption of data sharing agreements, with defined boundaries on where patients' health data would be held.

Data Sovereignty Question: Will health information stored in Cloud platforms be encrypted both at transit & rest?

Ideally, it is recommended that PHI health data is encrypted both at rest and transit, but based on decisions by whomever is responsible for managing the security of the application or cloud service.

De-Identification

De-Identification Question: What is happening in today's analytics business that has resulted in increased risk of re-identification of historical de-identified health data sets?

Re-identification risk - data science will eventually render any de-identification technique ineffective. Similar to challenges with encryption algorithms – we know that over time they will be cracked.

Ownership - lack of clarity around the ownership of, or rights to, de-identified data. Does it belong to the custodian, vendor or individual? Canada' regulators generally have concerns about organizations' ability to sustain due to ongoing expense to maintain their controls of de-identified data sets.

De-Identification Question: Is it permissible for Canadian HIT vendors providing de-identification services on behalf of health custodians?

"Yes", as an agent on behalf of health data custodian. However, there is no provision for the vendor to retain the resultant de-identified data sets, use for purposes of product research and development, AI and ML application development, testing.

We see future consideration of application of commercial synthetic health data generator solutions that may become a preferred option for avoiding need to de-identify PHI data. Synthetic health data is generated from real health data but is not real health data. It is "fake" health data that has the same statistical properties as the original real health data. Use cases include science R&D and software testing. Synthetic data can act as a proxy for the real data.

TECHNATION CA

Secondary Use

Secondary Use Question: Is it appropriate for Canadian HIT vendors to be included as participants in the community of health secondary users?

'Yes", high value in secondary use of health data for purposes of product research and development, AI and ML application development, testing.

Secondary Use Question: Has there been a Canadian jurisdiction that has demonstrated involvement of Canadian HIT vendors in collaboration with health custodians in finding value in trusted health system secondary use?

"Yes". What began as an shared initiative (Alberta Health Data Repository) between the Ministry of Health and Alberta Health Services, expanded with the leadership of Alberta Innovates and Health Data Collaboratory. The expanded vision included participation of vendors as contributors and users of shared provincial health data assets under restricted controls within common trusted environment.

General Data Protection Regulations (GDPR)

GDPR Question: What are the eight public/patient rights that GDPR has embraced for individuals and patients' data?

The GDPR regulations include eight public/patient data subject rights that include an individual's health data:

1. *The **right to be informed** – be transparent (including by maintaining a comprehensive privacy policy)*
2. *The **right of access** – Provide an individual access to a copy of their personal information*
3. *The **right of rectification** – Correct inaccurate personal information or allow user the ability to do so himself*
4. *The **right of erasure** – Delete an individual's personal information*
5. *The **right to restrict processing** – Temporarily stop processing someone's personal information in a specific way*
6. *The **right of data portability** – Provide an individual with an organized copy of their personal data in a commonly-used electronic format*
7. *The **right to object** – Stop processing an individual's personal data*
8. ***Rights related to automated decision-making** – Provide human intervention if you make automated decisions with highly significant impact.*

TECHNATION CA

GDPR Question: Are penalties for data breaches generally higher in the European Union jurisdictions as contrast to penalties applied in Canadian jurisdictions?

Fines under the GDPR can be very severe. At worst, they can reach $20million euros or 4 percent of a company's annual turnover (which ever is higher). Individuals can also bring a civil legal claim against a company that has violated their data protection rights.

Under Canada's PIPEDA legislation, the Office of the Privacy Commissioner (OPC) can investigate and demand information and conduct audits. The only monitor penalties specifically set out under PIPEDA are for failing to comply with an investigation of the OPC into a data breach. This can lead to fines ranging from $10,000 to $100,000 depending on the offense.

Digital Identity for Citizens

Digital Identity Question: Who should play the role of 3rd party auditor to verify if identity program is complaint federally, & provincially?

Provincial, Territory Government

Canada Health Infoway

How was Canada Health Infoway selected as the appropriate Federal Agency to develop the national service for Health Access Gateway and technology supports for digital identity?

Canada Health Infoway received federal funding envelope from Health Canada to pursue the design and implementation of the Health Access Gateway strategic program. Infoway's ACCESS Health program is promoting industry, health care providers, provinces, territories and Canadians to join in a shared ecosystem to provide Canadians online access. Goal of Health Access includes protection of individuals' personal health information through built-in privacy and security controls so that they can share it with family, caregivers and clinicians.