TECHNATION^CA

HEALTH PRIVACY AND SECURITY FRAMEWORK

TABLE OF CONTENTS

INTRODUCTION

The management of privacy and security have become priorities for government and business leaders responsible for the protection of sensitive health data and critical health infrastructure. Realizing the potential benefits of emerging technologies requires the establishment of a private and secure digital health infrastructure based on international standards for technology, data, and clinical management.

Recent privacy breaches and ransomware attacks have demonstrated how vulnerable our digital health systems are to compromise. Health data and systems are valuable assets that are targeted by malicious agents for financial gain or other advantage. Healthcare organizations and the technology companies that support them must be vigilant in ensuring that the appropriate privacy and security controls are in place.

TECHNATION Health Privacy and Security Framework

Privacy and Security in the Shadows of COVID-19

It is impossible to discuss issues of privacy and security in healthcare without acknowledging the global disruption driven by the COVID-19 pandemic. While privacy and security have always been issues of concern in healthcare, the COVID-19 crisis exacerbates the situation to levels not seen in modern history. Never has there been such a need to balance the rights of individuals against the need to protect the population from disease and death.

Responding to the pandemic will drive unprecedented levels of innovation as governments and public health authorities around the world seek solutions to problems that have never existed at this scale.

The following factors must be considered as we develop policies and standards to protect the privacy and security of personal health information and critical healthcare infrastructure.

Protection of Individual Privacy Rights

The Privacy Commissioners and Ombudsmen of Canada have issued a joint statement on privacy principles for contact tracing and similar apps[i]. The Commissioners recognize the privacy risks associated with these applications and offer specific guidance to organizations that plan to develop or use such applications.

Protection of Critical Infrastructure

The scale of the COVID-19 pandemic is placing a massive strain on the health care and public health systems in every country around the world. One of the goals of cybersecurity is to counteract all threats to critical infrastructure. This would include addressing the need for business continuity planning and the use of artificial intelligence (AI) and advanced analytics to effectively manage the crisis. We must ensure that our health care systems are not overwhelmed by the pandemic.

Protection of the Supply Chain

One of the early lessons of the pandemic crisis is the vulnerability of the supply chain for mission critical goods and services such as personal protective equipment (PPE), test kits, ventilators, vaccines, and therapeutics. The global nature of the supply chain and inadequacy of equipment stockpiles means few countries have the capability to respond to a rapidly advancing threat.

Pandemic Threat Response (PANTHR) De-Identification Project

The Government of Ontario has announced their Pandemic Threat Response Program to create a trusted, controlled data environment maintained under full control of the Ministry of Health to enable researchers and other health system users to access de-identified (pseudonymized) PHI with emphasis on access to pandemic related provincial data sets. "The Ontario government, in consultation with The Office of the Information and Privacy Commissioner of Ontario (IPC), is developing this new health data platform that 'will hold secure health data that will allow researchers to better support health system planning and responsiveness, including the immediate need to analyze the current COVID-19 outbreak'. PANTHR will gather de-identified data from publicly funded administrative health service records, such as physicians' claims to the Ontario Health Insurance Plan, drug claims submitted to the Ontario Drug Benefit Program and discharge summaries of hospital stays and emergency department visits."[ii]

Innovation to Advance Public Health Capabilities

Current approaches to public health management are inadequate to address challenges on a global scale. Innovation in digital health is required to enhance the capabilities of public health agencies in every country to respond to global pandemics. This will include testing, contact tracing, social distancing, vaccine, and therapeutic research. Special consideration must be given to the unique privacy risks associated with public health and the need to build and maintain public trust in public health systems.

An innovation that is gaining momentum for secondary use of health data is **syndromic surveillance,** that provides public health officials with a timely system for detecting, understanding, and monitoring health events. By tracking symptoms of patients in emergency departments—before a diagnosis is confirmed—public health can detect unusual levels of illness to determine whether a response is warranted.

Syndromic data can serve as an early warning system for public health concerns such as flu outbreaks and have been used in responses for opioid overdoses, vaping-associated lung disease, Zika virus infection, and natural disasters. Syndromic data has been demonstrated as an early sentinel for hot spot breakout of Coronavirus including an early March alert in New York City two weeks before the City called an emergency public health crisis. The US National Syndromic Surveillance Program (NSSP) is a collaboration among CDC, federal partners, local and state health departments, and academic and private sector partners who have formed a community of practice. They collect, analyze, and share electronic patient encounter data received from emergency departments, urgent and ambulatory care centers, inpatient healthcare settings, and laboratories.

APPROACH

TECHNATION Health plans to develop positions on a range of privacy and security policy issues over the course of the next year. Positions developed will address issues that are of concern to the vendor community, or areas where the vendor community can make substantial and meaningful contributions to the public debate.

For this first iteration, TECHNATION Health plans to address issues associated with:

- Cybersecurity;
- Data sovereignty;
- De-identification of health data;
- Secondary use of health data for R&D and innovation; and
- Alignment with the General Data Protection Regulation (GDPR).

In establishing the Privacy and Security Framework, TECHNATION Health consulted with the TECHNATION Health Advocacy Committee, Board, and privacy and security officers from member companies. TECHNATION Health members expressed the following needs with respect to the Framework:

- Need to build agility into the Framework to enable it to evolve and advance as legislation and standards change.

- Need to find ways to enable non-professional caregivers ensuring legislation is supportive to their needs and the needs of the patients.

- Need to be clear on who the target market/readership is for the paper and tailor content accordingly.

CYBERSECURITY

What is it?

Cybersecurity is the protection of information assets by addressing threats to information processed, stored, and transported by Internetworked information systems. Information assets include personal information, personal health information, intellectual property, trade secrets, security related information (e.g. passwords, security test results), and other information that could harm individuals and organizations if compromised.

What are the Issues?

Governance and compliance

Canadian privacy legislation gives very little guidance on security safeguards. Most enactments require reasonable security safeguards based on the sensitivity of the information in question.

Many large companies have undertaken due diligence exercises such as SOC2, ISO/IEC 27001, and HITRUST certifications. However, small and medium-sized enterprises (SMEs) are challenged to demonstrate that they are in compliance with acceptable practices for cybersecurity management.

In response to the challenges impacting SMEs, the Government of Canada has established the Canadian Centre for Cyber Security. Operated by the Communications Security Establishment, the Centre leads the government's response to cyber security events. It works with the private and public sectors to solve Canada's most complex cyber issues. It also helps to develop Canada's cyber security talent.

Efforts are also under way at the provincial level to promote cyber security. CyberNB is an agency of the Government of New Brunswick that is mandated to focus on growing the province's cybersecurity ecosystem. It works with business, academia and government to: facilitate growth and increase the talent pipeline through its Workforce Strategy; foster innovation to create an environment for secure critical infrastructure via its Innovation and Infrastructure Strategy; and secure business growth and customer trust through members of its ecosystem who offer cyber readiness, business process and common criteria certifications as part of its Trust and Compliance Strategy.

Standards

To be effective, the legislative and regulatory frameworks in Canada must be supported by national and international standards that define best practices and controls for cybersecurity management. Some of the standards that apply see to healthcare in

Canada, and Canadian Health information technology companies doing business in the United States include:

CSA Model Code for the Protection of Personal Information: Provides a foundation for privacy and security principles and controls. The code has been integrated as a schedule to the Personal Information Protection and Electronic Documents Act.

The ISO/IEC 27000 Series of Standards: A comprehensive suite of International standards widely adopted by healthcare organizations in Canada, United States, and Europe. Of note are the following:

- ISO/IEC 27001 – Information Security Management Systems Requirements
- ISO/IEC 27002 – Code of Practice for Information Security Controls
- ISO/IEC 27005 – information Security Risk Management
- ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO 27799 - Information security management in health using ISO/IEC 27002

The National Institute for Standards and Technology (NIST): Has published the NIST Special Publication 800 series of standards to address and support the security and privacy needs of US federal government information and information systems. Entities outside of the US federal government may voluntarily adopt NIST SP 800 – series publications, especially if they plan to do business with healthcare organizations in the United States. Guidance is provided on a wide variety of information security topics. Of note are the following:

- SP800-53 – Security and Privacy Controls for Information Systems and Organizations
- SP800-37 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- SP1800-1 - Securing Electronic Health Records on Mobile Devices
- SP 800-66 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

In addition to the SP800 series, NIST has published the **Cybersecurity Framework and Privacy Framework.**

Canada Health Infoway - Privacy and Security Voluntary Certification Requirements and Considerations for Digital Health Solutions

Certification

It can be difficult for HICT vendors to demonstrate compliance with privacy and security standards. Vendors are often confronted with numerous complex questionnaires issued by customers addressing privacy and security requirements as part of their own due diligence. Certification programs benefit both vendors and customers, where the assessment is completed once by a trusted independent evaluator and can be relied upon by all parties.

Several certification programs are available to healthcare technology vendors and healthcare organizations. They include:

SOC2 (Service Organization Controls 2): SOC2 is an auditing procedure established by the AICPA and CPA Canada to ensure that an organization's services and systems address the security, availability, processing integrity, confidentiality, and privacy of customer data.

ISO/IEC 27001 – Information security management systems – requirements: Certification of compliance with the requirements of ISO/IEC 27001 is conducted by certification bodies accredited by the International Accreditation Forum.

HITRUST CSF (Common Security Framework): The HITRUST Alliance is a privately held US company that established and maintains the HITRUST CSF. The HITRUST CSF is aligned with other national and international security standards and is widely adopted in US healthcare.

Canada Health Infoway Certification Program

CyberSecure Canada: Is a program of Innovation, Science and Economic Development (ISED) Canada designed to enable SMEs demonstrate compliance with minimum security standards. Certification audits are conducted by certification bodies accredited by the standards Council Canada. Certification marks are issued by ISED.

What are the Solutions?

TECHNATION Health Supports the alignment of Canadian privacy and security practices with national and international standards. The vendor community can play a national coordinating role in the governance of cyber security in healthcare.

The vendor community, as represented by TECHNATION Health, should define criteria for considering certification programs, including those that:

- Are national in scope.
- Are developed and maintained by competent authorities.
- Issue a recognizable certification mark.

The Canadian Centre for Cyber Security has published a set of Baseline Cyber Security Controls for SMEs[iii]. The Federal government has established CyberSecure Canada to certify compliance with the baseline cyber security controls.

For larger organizations, the ISO 27001 certification and/or SOC2 are appropriate. HITRUST may be required for vendors operating in the United States.

Recommendations for Cybersecurity

- **TECHNATION Health should endorse the Federal government's:**
  - **Baseline Cybersecurity Controls for SMEs; and**
  - **Cybersecure Certification Program.**
- **TECHNATION Health should work with the Canadian Centre of Cyber Security and Cybersecure Canada to promote the Baseline Cyber Security Controls and certification program to:**
  - **The TECHNATION membership;**
  - **The larger SME community;**
  - **The broader health sector; and**
  - **Information and privacy commissioners and ombudsmen.**
- **TECHNATION Health should promote ISO 27001 certification and/or SOC2 as the standard for large companies in healthcare.**
- **TECHNATION Health should lobby federal and provincial/ territorial jurisdiction to accept SOC2, 27001 and CyberSecure as evidence of security compliance for procurement actions.**

DATA SOVEREIGHNTY

What is it?

Data Sovereignty refers to geopolitical restrictions on the access, storage, and/or use of data. It is also known as data residency or data localization. Three Canadian provinces (BC, NS & NB) require that personal information (PI) and personal health information (PHI) held by public bodies be stored in or accessed from Canada only (exceptions apply). Alberta's Personal Information Protection Act (PIPA) requires that Individuals be notified when their data is stored outside of Canada (doesn't apply to health data). There are no restrictions in the remaining provinces, territories, or the federal government.

What are the Issues?

Data sovereignty has become a significant issue in many countries around the world. Nation states are recognizing the value of data for national security, law-enforcement, and economic purposes. In many parts of the Globe, countries are placing restrictions on the storage and use of data to ensure control over this valuable resource.

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.

Such restrictions may be impacted by International trade agreements such as the US Mexico Canada Trade Agreement (USMCA). Article 19.12 of the USMCA states, "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory." This prohibition on data sovereignty is mitigated to some extent by Article 19.8, Personal Information Protection, that requires the parties to, "adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade."

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.

Inconsistent rules within and across jurisdictions cause considerable confusion in the marketplace. In BC, NS & NB, restrictions apply to public bodies (i.e. Ministries of Health, Regional Health Authorities, hospitals). Restrictions do not apply to private medical clinics, labs, pharmacies, etc. Many health organizations outside of BC, NS & NB insist that data be stored in the province of residence, even though there is no legal requirement to do so.

What is the Solution?

The principal issues with respect to data sovereignty are the inconsistent rules applied by jurisdictions across Canada causing confusion in the marketplace. Current practices may be acceptable if these concerns are addressed through alignment of policies and practices and clear communications to stakeholders.

Recommendations for Data Sovereignty

- **TECHNATION Health should establish a policy position for custodian-controlled PHI, advocating for Canadian residency of data, but not constrained within a Province or Territory.**
- **TECHNATION health should establish a policy position for consumer-controlled health information advocating that such data not be subject to data residency restrictions.**
- **TECHNATION Health should approach those jurisdictions with no data sovereignty restrictions in place and ask that they issue guidance to the broader health sector confirming that the data sovereignty restrictions to not apply in that jurisdiction.**

DE-IDENTIFICATION

What is it?

"De-identification" is the general term for the process of removing personal information from a record or data set. De-identification protects the privacy of individuals because once de-identified, a data set is considered to no longer contain personal information. If a data set does not contain personal information, its use or disclosure cannot violate the privacy of individuals".[iv]

De-identification protects the privacy of individuals because once de- identified, a data set is considered to no longer contain personal information. De-identification is an essential process to enable secondary uses of PI and PHI for purposes including academic research, industrial R&D, and innovation. Most health privacy legislation allows a health information custodian (HIC) to de-identify PHI without the consent of the individual and constitutes a 'use' and not a 'disclosure'. The HIC may authorize or direct an agent or affiliate to de-identify the PHI on their behalf. The HIC may collect, use, or disclose de-identified information for any purpose. Private sector privacy legislation places no conditions on the de-identification of personal information. De-identification is considered a disposal option in some jurisdictions

Table 1. Examples of di-identification methods for health information data fields

Approach	Geographic	Alpha	Numeric
Reduction in detail	Reduce postal code to 1st 3 characters	Round birthdate to year Express dates relative to milestone date	
Suppression	Suppress geo-codes when they contain five observations or less	Suppress numbers when they contain five observations or less	Suppress alpha variables when they contain five observations or less
Substitution	If postal code is manipulated, then make certain that telephone area code is consistent	If health card number is manipulated, then make certain that the resultant number will pass checksum validation check	Select new names in same proportion as in use in public If surname is manipulated, then ensure that the new name has the same number of characters and ethnicity
Pseudonymization	Can be applied to most geo data	Can be applied to most alpha data	Can be applied to most numeric data

What are the Issues?

There is need standards for de-identification of data. *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.

What is the Solution?

In dealing with re-identification risk, each jurisdiction should apply a layered defense-in-depth strategy and acknowledge residual risk. Layered defenses could include de-identification techniques, Privacy Impact Assessments (PIAs) and Threat Risk Assessments (TRAs), privacy by design, contracts and agreements, regulatory oversight, and legal sanctions. To deal with the ownership issue, amend health sector and private sector privacy legislation to clarify the ownership of, and rights to, de-identified data.

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. Highlighting an open source example of the YODA Project, sponsored by Yale University and their Centre for Outcomes Research and Evaluation, has iteratively developed a model to make data available to researchers in a sustainable way, in which data sharing becomes a part of the clinical research enterprise of the future to not only increase access to clinical research data, but to promote its use to generate new knowledge[v].

Recommendations for De-Identification

- **TECHNATION Health should encourage the vendor community and health jurisdictions to apply a defense in depth strategy to the de-identification of health data.**
- **TECHNATION Health should encourage health jurisdictions to amend the privacy legislation to address the issues of ownership and rights to de-identified data.**

SECONDARY USE OF HEALTH DATA FOR INNOVATION AND RESEARCH

What is it?

The business models for many innovative companies includes the use of de-identified health data derived from PI or PHI for R&D or innovation purposes; Canadian Institute for Health Information (CIHI) has published expanded use cases for Secondary Health System Use[vi]. AI relies on machine learning (ML) and access to health data to enable the continuous improvement of algorithms and applications.

What are the Issues?

What are the processes and protocols for approving, permitting, or enabling the use of information for secondary purposes? Under most health privacy legislation, where a vendor is contracted to provide services to a HIC, the vendor can only use the health data in support of services delivered to the HIC and not for the purposes of the vendor. This rules out ML and other purposes that support innovation. There is great reluctance in the government and healthcare communities to monetize the use of health data for commercial purposes. Need to consider the needs of all potential consumers of health information for secondary purposes. Rapidly changing environment. Pandemic considerations – privacy legislation permits broad collection, use and disclosure of PHI for dealing with public health issues – but does not give carte blanch for snooping on your neighbors. Proprietary HIT systems often do not support the secondary purposes. Data is not readily accessible for secondary purposes.

What is the Solution?

Establish a process where the HIC could authorize the vendor to de-identify the PHI and then disclose the de-identified data to the vendor for ML and other innovative purposes. This should be documented in some form of agreement. This can be accomplished under present legislation in most jurisdictions. Amend privacy legislation to permit the use of de-identified health data by vendors for R&D and innovation. There should be safe data sets that can be used in secondary use settings by companies for research and innovation.

Recommendations for Secondary Use

- **TECHNATION Health should work with health jurisdictions to establish processes that will enable the secondary use of health data for R&D and innovation by HICT vendors.**
- **TECHNATION Health should facilitate dialogue between stakeholders promoting the art-of-the-possible and action steps**

ALIGNMENT WITH GDPR

What is it?

The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It confers new rights for data subjects such as the right to erasure (right to be forgotten), the right to data portability, and the right to object to processing. The GDPR also defines new responsibilities for data controllers and processors such as the requirement for data protection by design and default and for completion of data protection impact assessments.[vii]

What are the Issues?

The GDPR is becoming the global defacto standard for privacy and security. It is driving the evolution of privacy laws in most countries including Canada and the United States. Alignment with GDPR will help Canadian companies to build products for the Canadian market that can be exported globally.

What is the Solution?

In response the impact of the GDPR on healthcare in Canada:

- Jurisdictions should align, where appropriate, federal, provincial, and territorial privacy legislation with the GDPR.
- Where feasible, Canadian vendors and healthcare organizations should align business and technical requirements and processes with the GDPR.
- Coordinate and align international standards with the GDPR.

Recommendations for GDPR

- **TECHNATION Health should make representations to all jurisdictions recommending that, where appropriate, federal, provincial, and territorial privacy legislation should be amended to align with the GDPR.**
- **TECHNATION Health should publish a white paper to provide guidance to Canadian companies on practical measures to align with the GDPR.**

ACKNOWLEDGEMENTS

(20 individuals, from TECHNATION Health and 10 member organizations)

Co-Authors:

- Brendan Seaton, **Privacy Horizon**
- Susan Anderson, **TECHNATION Health**

Contribution of content and refinement and consensus building of recommendations by the following members of the TECHNATION Health Advocacy Committee and the working group task force:

- Aaron Berk, **KPMG** Advocacy co-chair
- Peter Jones, **Microsoft** Advocacy co-chair
- Philip Alcaidinho, **Meditech**
- Justin Armstrong, **Meditech**
- Ray Boisvert, **IBM**
- Susanne Flett, **HealthTech Consulting**
- Elaine Huesing, **TECHNATION Health**
- Patrick Lo, **Privacy Horizon**
- David Mohajer, **XaHive**
- Ashna Mohan, **XaHive**
- Tushar Pant, **IBM**
- Sem Ponnambalam, **XaHive**
- Garth Reid, **HP Enterprise**
- Tyson Roffey, **IBM**
- David Thomas, **Telus Health**
- Michael Whitt, **Bennett Jones LLP**

END NOTES

[i] https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/

[ii] https://www.bereskinparr.com/doc/panthr-ontario-s-commendable-use-of-de-identified-personal-health-information

[iii] https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

[iv] Emam, Khaled El. Guide to the De-identification of Personal Health Information. Boca Raton, FL: CRC Press, 2013.

[v] https://yoda.yale.edu/welcome-yoda-project

[vi] https://www.cihi.ca/en/hsu_vision_report_en.pdf

[vii] https://gdpr.eu/