

TECHNATION CA

HEALTH ADVOCACY PRIVACY AND SECURITY FRAMEWORK

UPDATE FOR 2024

Table of Contents

INTRODUCTION 3
APPROACH 4
CYBERSECURITY 5
DATA SOVEREIGNTY 9
DE-IDENTIFICATION 11
SECONDARY USE OF HEALTH DATA FOR INNOVATION AND RESEARCH 14
ALIGNMENT WITH GDPR 15
AI FRAMEWORK 16
AI GOVERNANCE 19
ACKNOWLEDGEMENTS 21
END NOTES 21

INTRODUCTION

Privacy and security management have become priorities for government and business leaders responsible for protecting 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.

The recent privacy breaches and ransomware attacks have starkly illustrated the vulnerability of our digital health systems. It's important to remember that health data and systems are not just vulnerable, they are also highly valuable assets that malicious agents target for financial gain or other advantages.

Healthcare organizations and the technology companies that support them must maintain a constant state of vigilance. It's not enough to ensure that the appropriate privacy and security controls are in place; they must also be regularly reviewed and updated to keep up with the evolving threat landscape.

Privacy and Security in the Transition to Post-COVID Era

The COVID-19 pandemic catalyzed a global shift towards digital health, leading governments and businesses to rapidly implement data protection and cybersecurity measures. This urgent response to the pandemic demonstrated the critical importance of robust privacy and cybersecurity practices in protecting health data against emerging threats.

As we transition into the post-COVID era, the momentum gained in enhancing data protection and cybersecurity measures must be sustained. The valuable lessons learned during the pandemic should serve as a guide for ongoing efforts to secure digital health technologies and protect sensitive health information.

The integration of digital health technologies into healthcare delivery is an irreversible trend. Telehealth, electronic health records (EHRs), and AI-driven health tools have become pillars of modern healthcare, making the protection of digital health data more critical than ever. In this evolving landscape, the focus on privacy and security must be dynamic and capable of adapting to new technologies and threats.

Continued diligence in privacy and cybersecurity is essential to safeguarding patients' and healthcare providers' trust and confidence in digital health systems. This requires a commitment to ongoing investment in security infrastructure, the development of new policies and standards, and the promotion of a culture of security awareness across the healthcare sector.

In the post-COVID era, our collective responsibility is to ensure that a strong foundation of privacy and cybersecurity supports the advancements in healthcare technology made during the pandemic. By maintaining our guard and fostering innovation within a secure and private framework, we can ensure that digital health technologies continue to enhance healthcare delivery without compromising the integrity and confidentiality of health data.

APPROACH

TECHNATION Health plans to develop positions on a range of privacy and security policy issues over the next year. The positions will address issues that concern 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;
- AI Framework;
- AI Governance; 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, the Health 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 a critical practice that aims to safeguard information assets against various threats that may arise from the use of interconnected information systems. These information assets could include personal information, personal health information, intellectual property, trade secrets, security-related information, such as passwords and security test results, and other sensitive information that could potentially cause harm to individuals and organizations if compromised.

Cybersecurity is a crucial practice that ensures the confidentiality, integrity, and availability of information assets, thereby protecting individuals and organizations from the negative consequences of cyber threats.

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 comply with acceptable cybersecurity management practices.

The Government of Canada has established the Canadian Centre for Cyber Security in response to the challenges impacting SMEs. 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 and helps develop Canada's cyber security talent.

Efforts are also underway 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, Canada's legislative and regulatory frameworks must be supported by national and international standards that define best practices and controls for cybersecurity management. Some of the standards that apply 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: This code provides a foundation for privacy and security principles and controls. It 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, the 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): It 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.**

Certification

It can be challenging for Health Information and Communication Technology (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 bodies accredited by the International Accreditation Forum conduct compliance certification with ISO/IEC 27001 requirements.

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.

CyberSecure Canada: This is a program of Innovation, Science and Economic Development (ISED) Canada designed to enable SMEs to 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 aligning Canadian privacy and security practices with national and international standards. The vendor community can play a national coordinating role in governing 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. 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/or CyberSecure as evidence of security compliance for procurement actions.

DATA SOVEREIGNTY

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. Currently, Nova Scotia is the only Canadian province that requires that personal information (PI) and personal health information (PHI) held by public bodies be stored in or accessed from Canada only (exceptions apply).

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 recognize data's value 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. Since that time, British Columbia and New Brunswick have revised their legislation to remove the restriction.

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, which 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.

These companies have already made significant investments in 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 NS, 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 NS 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 issue with respect to data sovereignty is the inconsistent rules applied by jurisdictions across Canada, which causes confusion in the marketplace. Current practices may be acceptable if these concerns are addressed through the alignment of policies and practices and clear communications with 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 jurisdictions with no data sovereignty restrictions in place and ask that they issue guidance to the broader health sector confirming that the restrictions do 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 essential to enable secondary uses of PI and PHI for 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 de-identification methods for health information data fields

Approach	Geographic	Alpha	Numeric
Reduction in detail	Reduce postal code to first three 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

Approach	Geographic	Alpha	Numeric
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 a 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 a need for 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's 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?

When it comes to managing the risk of re-identification, it is recommended that each jurisdiction adopt a layered defense-in-depth strategy while acknowledging the possibility of residual risk. The strategy can include various approaches such as de-identification techniques, Privacy Impact Assessments (PIAs) and Threat Risk Assessments (TRAs), privacy by design, contracts and agreements, regulatory oversight, and legal sanctions. To address the issue of data ownership, it is suggested that health sector and private sector privacy legislation be amended to clarify the ownership of and rights to de-identified data.

In the future, it is possible that commercial synthetic health data generator solutions may become a popular alternative to de-identification of PHI data. Synthetic health data is generated from real health data, but it is not real health data. It is a "fake" version of health data that has the same statistical properties as the original real health data. Synthetic data can be used as a proxy for real data, making it useful for science R&D and software testing. An open-source example of this is the YODA Project, which is sponsored by Yale University and its Center for Outcomes Research and Evaluation. They have developed a model that makes data available to researchers in a sustainable way, where data sharing becomes a part of the clinical research enterprise f the future. This not only increases access to clinical research data but also promotes the use of data to generate new knowledge[vi]. The Canadian Anonymization Network (CANON) has been established to serve as a not-for-profit network of data custodians across various sectors. Its primary objective is to promote anonymization for privacy-respectful data usage.

Recommendations for De-Identification

- TECHNATION Health should encourage the vendor community and health jurisdictions to apply an in-depth defense strategy to the de-identification of health data.
- TECHNATION Health should encourage health jurisdictions to amend their privacy legislation to address the issues of ownership and rights to de-identified data.
- TECHNATION Health should address the technical challenges and data ownership/rights concerns associated with de-identifying data on behalf of the HIC. It should develop robust solutions to overcome these challenges and ensure data ownership and rights are clearly defined and protected. This may involve collaborating with relevant stakeholders, such as legal experts and technology specialists, to devise a comprehensive strategy for addressing these issues.

SECONDARY USE OF HEALTH DATA FOR INNOVATION AND RESEARCH

What is it?

Many innovative companies' business models include using de-identified health data derived from PI or PHI for R&D or innovation purposes; the Canadian Institute for Health Information (CIHI) has published expanded use cases for Secondary Health System Use. 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. We 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 blanche for snooping on your neighbours. Proprietary HICT systems often do not support 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 companies can use in secondary-use settings 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 set of rules under EU law that govern data protection and privacy in the European Union and the European Economic Area. It comes with various rights for data subjects, such as the right to be forgotten, the right to data portability, and the right to object to processing. The GDPR also defines new obligations for data controllers and processors, including the requirement for data protection by design and default and for completion of data protection impact assessments. Quebec passed Law 25, also known as Bill 64, which is a law that significantly updates the province's privacy legislation and governs the protection of personal information in Quebec. This privacy law is closely aligned with GDPR.

What are the Issues?

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

What is the Solution?

In response to 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 providing guidance to Canadian companies on practical measures to comply with the GDPR.

AI FRAMEWORK

What is it?

An AI Framework is a comprehensive set of guidelines, standards, and best practices that provide a roadmap for the ethical and responsible development, deployment, and management of artificial intelligence technologies in the healthcare sector. The framework ensures that AI solutions align with the needs and expectations of patients, healthcare providers, and other stakeholders. It emphasizes the importance of data privacy and security, as well as the need to enhance the delivery of healthcare and improve patient outcomes using AI. The framework provides guidance on issues such as data quality, algorithm transparency, and explainability, and it promotes a culture of collaboration and accountability among all stakeholders involved in the development and deployment of AI technologies in healthcare. By following the AI Framework, healthcare providers can ensure that they are using AI safely, effectively, and ethically, and they can build trust with patients and other stakeholders in the healthcare ecosystem.

What are the Issues?

The implementation of AI in healthcare will bring numerous benefits, such as improved diagnostic accuracy, better patient outcomes, and reduced human error. However, it has also raised several concerns that need to be addressed. One of the primary concerns is ethical considerations. Ensuring that AI-powered solutions respect patient rights and privacy while handling sensitive health information is crucial. This includes ensuring that the data collected is used only for the intended purpose and with the patient's consent.

Another issue that needs to be addressed is the inherent biases in AI algorithms. These biases can lead to unequal treatment or outcomes, particularly in the case of vulnerable populations. Identifying and rectifying these biases is essential to ensure that the AI algorithms are fair and just for everyone.

Furthermore, data quality and management are crucial factors to consider when implementing AI in healthcare. The integrity and security of data used in AI applications are of paramount importance. Ensuring that the data collected is accurate and reliable is crucial for the accuracy of the AI algorithms. Additionally, ensuring that the data is protected from cyber-attacks and breaches is vital to maintaining patient privacy and confidentiality.

What is the Solution?

Establishing a strong governance structure is crucial to ensure the responsible and ethical use of AI. This structure should include oversight bodies that can regulate and monitor the use of AI and its impact on society. Additionally, it's essential to implement standards for transparency, explainability, and accountability in AI algorithms and decision-making processes. This means that the developers of AI systems should provide clear explanations for their algorithms' decisions and be held accountable for any negative consequences that arise from their use.

A multi-stakeholder approach is necessary to address the bias in AI systems. This means involving various stakeholders, including civil society, academia, governments, and the private sector, to ensure that diverse and inclusive AI development practices are adopted. This approach can help identify and address any bias in AI systems and ensure that they are inclusive and equitable for all members of society.

Recommendations

- TECHNATION Health should advocate for the development of a national AI framework for healthcare that aligns with international standards. The framework should be designed to regulate and monitor the use of AI in healthcare, ensuring that it is aligned with ethical principles and does not compromise the privacy and security of patients' information.
- Encourage member organizations to adopt AI ethics guidelines and provide their staff with ongoing AI education and training opportunities.
- To ensure that AI governance structures are inclusive and transparent, TECHNATION Health should collaborate with regulatory bodies, healthcare providers, and patients. The organization should work with these stakeholders to develop robust governance structures that ensure the responsible use of AI in healthcare.

AI GOVERNANCE

What is it?

AI Governance in healthcare is a crucial aspect of managing and overseeing the use of AI technologies in the healthcare industry. It encompasses a wide range of systems, policies, and procedures designed to ensure that AI is used ethically, safely, and in compliance with legal and regulatory standards. The main objectives of AI Governance in healthcare are to align the use of AI with healthcare objectives and patient safety, ensure that data privacy and security are maintained, and promote transparency and accountability in the use of AI. This involves developing clear guidelines for the use of AI, establishing protocols for monitoring and evaluating AI systems, and implementing training programs to ensure that healthcare professionals are equipped to use AI technologies safely and effectively. AI Governance in healthcare is a complex and evolving field, and it requires ongoing attention and adaptation to keep pace with advancements in AI technologies and changing healthcare needs.

What are the Issues?

In the healthcare industry, the use of artificial intelligence (AI) is becoming increasingly prevalent as it offers numerous benefits, such as improved diagnosis, treatment, and patient outcomes. However, with all new technology comes challenges and there are several issues that need to be addressed to ensure the safe and effective use of AI in healthcare.

- Regulatory compliance is a significant issue in healthcare AI. The complex and ever-changing landscape of healthcare regulations presents a challenge for developers, vendors, and healthcare providers, who must ensure that their AI systems comply with all applicable laws and regulations. This includes issues related to data privacy, security, and transparency.
- Accountability and oversight are crucial when it comes to AI in healthcare. The use of AI systems can significantly impact patient outcomes and decision-making processes, and it is essential to establish clear responsibilities for AI outcomes and decision-making processes. This includes understanding who is responsible for decisions made by AI systems and how to ensure that these decisions are fair, transparent, and free from bias.
- Integration with existing healthcare systems is another issue that needs to be considered when implementing AI in healthcare. It is essential to ensure that AI tools complement and enhance current practices without disrupting care delivery.

This requires careful planning and coordination between healthcare providers and technology vendors to ensure that AI systems are integrated smoothly and efficiently into existing healthcare systems.

What is the Solution?

- Develop comprehensive governance frameworks that detail policies for AI development, deployment, and monitoring.
- Create cross-functional oversight committees to ensure ongoing evaluation of AI technologies against ethical, legal, and operational standards.
- Foster partnerships between technology providers, healthcare institutions, and regulatory agencies to streamline AI integration and compliance efforts.

Recommendations

- TECHNATION Health should facilitate discussions on AI governance models and share best practices among members.
- Promote the adoption of standardized AI governance tools and metrics for performance and impact assessment.
- Advocate for the establishment of legal and regulatory guidelines specific to the use of AI in healthcare.

ACKNOWLEDGEMENTS

Lead Author:

- Patrick Lo, **Privacy Horizon Inc.**

We would like to thank and acknowledge the members of TECHNATION's Health Advocacy Committee and Health Board of Directors for their contribution of content, refinement and consensus building to the 2024 Framework update.

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/