



# HEALTH PRIVACY AND SECURITY FRAMEWORK

UPDATE FOR 2026

## Table of Contents

|                                                               |    |
|---------------------------------------------------------------|----|
| INTRODUCTION .....                                            | 3  |
| APPROACH.....                                                 | 4  |
| CYBERSECURITY .....                                           | 6  |
| DATA SOVEREIGNTY .....                                        | 13 |
| DE-IDENTIFICATION.....                                        | 16 |
| SECONDARY USE OF HEALTH DATA FOR INNOVATION AND RESEARCH..... | 19 |
| ALIGNMENT WITH GDPR.....                                      | 21 |
| RESPONSIBLE AI GOVERNANCE IN HEALTHCARE .....                 | 22 |
| MEASURING MATURITY AND OUTCOMES .....                         | 26 |
| ACKNOWLEDGEMENTS .....                                        | 26 |
| END NOTES.....                                                | 26 |

## INTRODUCTION

Privacy, security, and trust are foundational to safe, resilient, and effective healthcare delivery. As digital ecosystems expand to include artificial intelligence, hybrid cloud environments, connected medical devices, and interoperable data platforms, healthcare organizations must adopt a proactive, risk-based approach to protecting patient data and ensuring continuity of care.

Targeted 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.

Cybersecurity and privacy are no longer solely compliance functions; they are critical components of patient safety and operational resilience. Healthcare organizations must do their due diligence to prevent breaches but also ensure they can maintain safe clinical operations during disruptions, including cyber incidents, system outages, and infrastructure failures.

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. Within this changing environment, the emphasis on security and privacy needs to remain dynamic, concurrently adapting to emerging threats and new technologies.

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.

## 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;
- Responsible AI governance in healthcare;
- 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:

- Align with national digital health standards, including **Canada Health Infoway's Connected Care Trust Framework (CCTF)**, to support a federated "trust once, reuse many times" model for health data exchange.
- Anchor health AI principles within Canada's National Artificial Intelligence Strategy: AI for All, ensuring national AI missions (including the \$200M healthcare adoption commitment) are met with robust privacy and security safeguards.
- 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.

- Define clear expectations for operational maturity, including cybersecurity resilience, AI governance lifecycle management, and ecosystem-wide risk management.
- Provide actionable guidance for vendors and healthcare organizations beyond policy alignment.
- Healthcare organizations should encourage appropriate transparency, data provenance, source attribution, and traceability in the technologies they adopt, proportionate to the technology's intended use and level of risk, while recognizing that reasonable assurance may be achieved through documentation, auditability, validation, and other controls without requiring disclosure of proprietary intellectual property or underlying technical implementation.

## 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.

Cybersecurity in healthcare must be treated as a patient safety function. Disruptions to systems, data integrity, or availability can have direct clinical consequences, requiring organizations to prioritize resilience alongside prevention.

### ***Cyber Resilience and Continuity of Care***

Healthcare organizations must implement comprehensive resilience strategies to maintain care delivery during cybersecurity incidents or system outages. This includes:

- Documented downtime procedures and manual fallback workflows for critical clinical functions
- Regular tabletop exercises and simulation-based testing
- Redundant communication mechanisms, such as secure messaging alternatives
- Integration of cybersecurity into enterprise risk and emergency preparedness programs

### ***Identity and Access Security***

Identity security represents a primary control point in healthcare environments. Organizations should adopt:

- Phishing-resistant multi-factor authentication where feasible
- Least privilege and role-based access control
- Privileged access governance and monitoring
- Regular access reviews and timely deprovisioning
- Secure controls for shared clinical workstations and mobile devices

### ***Third-Party and Supply Chain Risk Management***

Healthcare organizations increasingly rely on cloud providers, AI vendors, and ecosystem partners. Organizations should:

- Define minimum security and privacy requirements for all vendors
- Require independent assurance, such as SOC2 or ISO, proportionate to risk
- Establish contractual obligations for breach notification and data handling
- Ensure visibility into subcontractors and data flows
- Assess operational dependencies affecting continuity of care

### ***Physical and Clinical Environment Security***

Physical safeguards remain a critical component of protecting health information:

- Control physical access to clinical areas, systems, and devices
- Use privacy screens and positioning to prevent unauthorized viewing
- Enforce clean-desk and secure document handling practices
- Regularly audit badge and facility access
- Apply network segmentation to isolate clinical systems and connected devices

### ***Connected Medical Device Cybersecurity***

Connected medical devices and clinical technologies represent a growing healthcare-specific cybersecurity risk. Organizations should maintain accurate device inventories, understand clinical dependencies, and coordinate security controls with biomedical engineering, clinical engineering, IT, security, procurement, and manufacturers.

- Maintain inventories of connected, unmanaged, agentless, and unpatchable clinical devices
- Apply patching where feasible and compensating controls where patching is not possible
- Coordinate vulnerability disclosure, remediation, and lifecycle support with manufacturers
- Use segmentation or microsegmentation to limit lateral movement without disrupting clinical workflows
- Continuously monitor clinical device traffic, dependencies, and anomalous behaviour

### ***Workforce Security and Culture***

Technology alone cannot mitigate cybersecurity risk. A strong security culture is required:

- Implement ongoing, practical training, including micro-learning and simulations
- Conduct phishing and social engineering testing
- Designate security champions within departments
- Establish clear escalation and reporting protocols

- Include vendors and partners in security awareness efforts

### **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

**United States federal healthcare cybersecurity guidance:** Organizations operating in or serving the U.S. healthcare market should align security programs with the current federal posture, including NIST Cybersecurity Framework 2.0, NIST SP 800-66 Revision 2, and the HHS Office for Civil Rights proposed HIPAA Security Rule modernization issued December 27, 2024.

NIST Cybersecurity Framework 2.0 is now the current NIST baseline for cybersecurity risk management. It adds a Govern function that elevates cybersecurity to an enterprise risk, accountability, policy, oversight, and supply-chain governance issue rather than a purely technical control set.

Relevant U.S. references include:

- 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 Revision 2 — Implementing the Health Insurance Portability and Accountability Act Security Rule: A Cybersecurity Resource Guide, published in February 2024 and superseding Revision 1.
- NIST Cybersecurity Framework 2.0, including the Govern, Identify, Protect, Detect, Respond, and Recover functions.

The December 27, 2024 HHS OCR HIPAA Security Rule Notice of Proposed Rulemaking, which remains proposed unless and until finalized, and emphasizes stronger written policies, risk analysis, testing, resilience, and modern cybersecurity safeguards for electronic protected health information. Together, these references support a more evidence-based security posture focused on governance, asset visibility, documented policies and procedures, recurring review, vulnerability management, incident response, recovery capability, and demonstrable control effectiveness.

### **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 governments:
  - 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.
- TECHNATION Health should promote cyber resilience planning and simulation-based preparedness.
- TECHNATION Health should advocate for strong identity and access controls across the healthcare sector.
- TECHNATION Health should promote structured third-party and ecosystem risk management practices.
- TECHNATION Health should emphasize workforce training and culture as core components of cybersecurity programs.
- TECHNATION Health should promote connected medical device cybersecurity practices, including device inventories, manufacturer coordination, vulnerability management, segmentation, and continuous monitoring

## DATA SOVEREIGNTY

### What is it?

Data sovereignty refers to legal, policy, contractual, or geopolitical requirements affecting where data is stored, where it may be accessed from, and how foreign lawful access risk is managed. It should be distinguished from data residency, cross-border transfer governance, and overall privacy and security assurance.

Nova Scotia has historically been the principal Canadian jurisdiction requiring certain personal information and personal health information held by public bodies to be stored in or accessed from Canada, subject to exceptions. However, Nova Scotia's regime is in transition under a modernized FOIPOP framework expected to come into force on April 1, 2027, with PIIDPA to be repealed.

Even where strict residency requirements do not apply, organizations should not characterize cross-border processing as unrestricted. Canadian privacy law, regulator guidance, procurement requirements, and AI governance expectations increasingly require transfer assessments, documented risk analysis, transparency, contractual controls, and safeguards proportionate to the sensitivity and use of the information.

### 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.

Data residency requirements should be distinguished from overall security and privacy assurance. Residency alone does not guarantee protection; organizations must focus on lawful access, governance, transparency, and appropriate safeguards regardless of data location.

For Canadian public-sector AI, organizations should also distinguish general AI governance from federal administrative decision-making requirements. The Government of Canada Directive on Automated Decision-Making, updated June 24, 2025, remains the practical federal reference for automated systems that make or support administrative decisions, with requirements for transparency, accountability, fairness, impact assessment, monitoring, and recourse.

## **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 techniques used to reduce the likelihood that information can be linked to an identifiable individual. Whether information is considered de-identified, anonymized, or still personal information depends on the governing statute, context, intended use, available safeguards, and residual re-identification risk.

De-identification can reduce privacy risk and support secondary uses of health information, but it does not eliminate governance, contractual, security, transparency, or accountability obligations.

Health privacy statutes may permit custodians to de-identify personal health information, and may allow agents or service providers to perform de-identification on behalf of custodians under appropriate authority and controls. However, the permitted use, disclosure, retention, commercialization, or further processing of de-identified data should be assessed under the applicable statute, contractual arrangements, ethical expectations, and residual risk profile. Organizations should avoid treating de-identification as a blanket authorization for any purpose.

*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<br><br>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<br><br>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?

De-identification should be treated as a continuous risk management process rather than a one-time technical activity. Organizations must manage residual re-identification risk through governance, access controls, contractual restrictions, and ongoing monitoring.

*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.

De-identified and synthetic data usage should be governed through defined permitted-use frameworks, validation standards, and auditability requirements.

## 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 of the future. This not only increases access to clinical research data but also promotes the use of data to generate new knowledge<sup>vi</sup>. 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.

Secondary use of health data must be governed by clear authorization models and transparency mechanisms:

- Defined permissible uses, such as research, innovation, and AI training
- Explicit agreements between custodians and vendors
- Separation of clinical, research, and commercial use cases
- Transparency to patients and stakeholders
- Auditability and oversight mechanisms

### What is the Solution?

Establish an authorization model under which the HIC may permit de-identification and secondary use only for defined purposes, supported by documented agreements,

privacy and security assessments, auditability, role-based access, retention limits, and controls preventing unauthorized re-identification or repurposing. Where legislative amendments are considered, they should clarify permissible uses, rights, accountability, and oversight for de-identified and synthetic health data rather than creating an unrestricted category of data use.

Trusted safe data environments, governed data access models, and validated synthetic data sets can support research and innovation while maintaining clear permitted-use, retention, audit, and accountability controls.

### **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?

Global privacy principles—such as privacy by design, transparency, accountability, and individual rights—are increasingly shaping healthcare regulation. Canadian frameworks should align with these principles while adapting to national and sector-specific requirements.

### 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.

## RESPONSIBLE AI GOVERNANCE IN HEALTHCARE

### What is it?

Responsible AI governance ensures that artificial intelligence systems are developed, deployed, and managed in a manner that is safe, ethical, transparent, and aligned with healthcare objectives and patient outcomes.

### AI Governance Lifecycle Model

Organizations should adopt a lifecycle-based governance approach:

1. **Intake and Use Case Approval:** Define purpose, scope, and expected outcomes.
2. **Data and Privacy Review:** Assess data quality, privacy risks, and consent considerations.
3. **Risk and Ethics Assessment:** Evaluate bias, fairness, explainability, and safety.
4. **Implementation Controls:** Ensure human oversight and integration into clinical workflows.
5. **Deployment and Monitoring:** Track performance, outcomes, and unintended impacts.
6. **Continuous Revalidation:** Periodically reassess models and retrain where needed.

### Current AI Governance Expectations in Healthcare (U.S. and Canada)

Healthcare AI governance is becoming more concrete and sector-specific. In the United States, ONC's HTI-1 Final Rule establishes transparency expectations for predictive algorithms embedded in certified health IT and supports clinical assessment of whether such tools are fair, appropriate, valid, effective, and safe. It also adopts USCDI Version 3 as the new baseline in the ONC Health IT Certification Program as of January 1, 2026.

In Canada, healthcare AI governance is being shaped by federal privacy regulator priorities, provincial health-sector guidance, AI-scribe guidance, public-sector automated decision-making requirements, and Health Canada's expectations for machine-learning-enabled medical devices, and Canada's National Artificial Intelligence Strategy: AI for All. Released as a whole-of-government framework, AI for All establishes national priorities around safe and trustworthy AI, sovereign compute infrastructure, AI literacy, and dedicated sector missions—including a \$200 million healthcare mission aimed at accelerating AI adoption in diagnostics and patient care. Aligning health AI deployment with AI for All ensures that vendor innovation supports national productivity while upholding rigorous data governance, transparency, and safety standards. Organizations

should treat AI governance as a lifecycle discipline supported by privacy impact assessments, vendor due diligence, documented accountability, human oversight, monitoring, and incident response.

- Transparency and explainability for clinical users, patients, and oversight bodies
- Human oversight and clear responsibility for clinical or operational decisions
- Vendor due diligence, contractual controls, and audit rights
- Data provenance, training-data legality, consent considerations, and retention controls
- Bias, accuracy, performance, drift, and safety monitoring after deployment
- AI-specific privacy impact assessments, risk assessments, and security assessments
- Breach, safety, model failure, and incident-response procedures
- Decommissioning, retraining, and data-disposal controls

## **Healthcare AI Product Categories**

AI governance should distinguish between general-purpose or administrative AI, clinical decision support, and machine-learning-enabled medical devices. The risk, evidence, oversight, validation, and regulatory expectations differ across these categories.

For machine-learning-enabled medical devices in Canada, Health Canada's April 2026 pre-market guidance emphasizes good machine learning practice, risk management, data selection and management, testing and evaluation, clinical validation, transparency, post-market monitoring, and predetermined change control plans for planned model changes.

## **AI Governance Principles**

AI governance should be grounded in the following principles:

- Safety and patient protection
- Accountability and defined responsibility
- Transparency and explainability
- Privacy and data protection
- Interoperability and system integration

- Continuous monitoring and improvement

### **Recommendations for Responsible AI Governance**

- TECHNATION Health should align healthcare AI initiatives with Canada's National Artificial Intelligence Strategy: AI for All, leveraging national AI healthcare missions to accelerate trusted vendor adoption, sovereign compute utilization, and workplace AI literacy.
- TECHNATION Health should advocate for alignment with Canada Health Infoway's Connected Care Trust Framework (CCTF) to ensure that AI-driven applications integrate seamlessly and securely into Canada's broader digital health interoperability ecosystem.
- TECHNATION Health should promote lifecycle-based AI governance frameworks.
- TECHNATION Health should advocate for ongoing monitoring and revalidation of AI systems post-deployment.
- TECHNATION Health should encourage multidisciplinary oversight structures that include clinical, privacy, security, legal, data governance, patient safety, and operational stakeholders.
- TECHNATION Health should support workforce readiness and AI literacy programs.
- TECHNATION Health should promote AI-specific privacy impact assessments, vendor due diligence, data provenance reviews, and retention/decommissioning controls.
- TECHNATION Health should distinguish general-purpose AI, clinical decision support, and regulated machine-learning-enabled medical devices in guidance, procurement, and assurance expectations.
- 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.

- 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.

## MEASURING MATURITY AND OUTCOMES

Organizations should adopt maturity models and measurable indicators to assess privacy and security capabilities, including:

- Cybersecurity resilience maturity
- AI governance maturity
- Data governance and interoperability readiness
- Workforce training and awareness metrics

## ACKNOWLEDGEMENTS

**Lead Author:**

- \_\_\_\_\_.

**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 2026 Framework update.**

## END NOTES

---

- i [https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d\\_20200507/](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](https://www.cihi.ca/en/hsu_vision_report_en.pdf)
- vii <https://gdpr.eu/>
- viii HHS Office for Civil Rights, “HIPAA Security Rule NPRM,” December 27, 2024. <https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/index.html>
- ix HHS Office for Civil Rights, “HIPAA Security Rule Notice of Proposed Rulemaking to

Strengthen Cybersecurity for Electronic Protected Health Information,” Fact Sheet, December 27, 2024. <https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html>

- x National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” February 26, 2024. <https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20>
- xi National Institute of Standards and Technology, “Cybersecurity Framework,” CSF 2.0 resources and quick-start materials. <https://www.nist.gov/cyberframework>
- xii National Institute of Standards and Technology, SP 800-66 Revision 2, “Implementing the Health Insurance Portability and Accountability Act Security Rule: A Cybersecurity Resource Guide,” February 2024. <https://csrc.nist.gov/pubs/sp/800/66/r2/final>
- xiii Office of the National Coordinator for Health Information Technology, “HTI-1 Final Rule,” algorithm transparency, information sharing, and USCDI Version 3 baseline. <https://www.healthit.gov/regulations/hti-rules/hti-1-final-rule/>
- xiv Federal Register, “Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing,” January 9, 2024. <https://www.federalregister.gov/documents/2024/01/09/2023-28857/health-data-technology-and-interoperability-certification-program-updates-algorithm-transparency-and>
- xv Office of the Privacy Commissioner of Canada, “Privacy and artificial intelligence (AI).” <https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/>
- xvi Office of the Privacy Commissioner of Canada, “Principles for responsible, trustworthy and privacy-protective generative AI technologies,” December 7, 2023. [https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd\\_principles\\_ai/](https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/)
- xvii Information and Privacy Commissioner of Ontario, “AI Scribes: Key Considerations for the Health Sector,” January 28, 2026. <https://www.ipc.on.ca/en/resources/ai-scribes-key-considerations-health-sector>
- xviii Office of the Information and Privacy Commissioner for British Columbia, “PIPA and AI scribes: best practices for healthcare organizations in BC,” January 2026. <https://www.oipc.bc.ca/documents/guidance-documents/3082>
- xix Office of the Information and Privacy Commissioner for British Columbia, “OIPC releases guidance on protecting patient privacy when using AI scribes,” January 28, 2026. <https://www.oipc.bc.ca/documents/news-releases/3083>
- xx Health Canada, “Pre-market guidance for machine learning-enabled medical devices,” April 1, 2026. <https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/pre-market-guidance-machine-learning-enabled-medical-devices.html>

- <sup>xxi</sup> Treasury Board of Canada Secretariat, “Directive on Automated Decision-Making,” updated June 24, 2025. <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>
- <sup>xxii</sup> Government of Nova Scotia, “Province Introduces Modernized Access, Privacy Legislation,” September 26, 2025. <https://news.novascotia.ca/en/2025/09/26/province-introduces-modernized-access-privacy-legislation>
- <sup>xxiii</sup> CanLII, Freedom of Information and Protection of Privacy Act, SNS 2025, c 13. <https://www.canlii.org/en/ns/laws/astat/sns-2025-c-13/latest/sns-2025-c-13.html>
- <sup>xxiv</sup> HIMSS, healthcare cybersecurity and medical device security resources. <https://www.himss.org/>