Canada's Drug and Health Technology Agency

CDA-AMC Health Technology Review

Implementation Review for Artificial Intelligence-Enabled Medical Devices: Supporting Information

August 2024

Implementation Review

Table of Contents

List of Included Guidance

The citations provided in this list are the publications included in this implementation review.

Australian Government (2024) Artificial Intelligence (AI) and medical device software https://www.tga.gov.au/how-we-regulate/manufacturing/manufacture-medical-device/manufacture-specific-types-medical-devices/software-based-medical-devices/artificial-intelligence-ai-and-medical-device-software

Registered Nurses' Association of Ontario (2024) Clinical Practice in a Digital Health Environment. https://rnao.ca/bpg/guidelines/clinical-practice-digital-health-environment.

Canada Health Infoway (2023) Digital Health Solutions Privacy and Security Guideline Canada Health Infoway Digital Health Solutions Privacy & Security Guideline (infoway-inforoute.ca)

Canada Health Infoway (2023) Toolkit for Implementers of Artificial Intelligence in Health Care: Toolkit for AI Implementers | Canada Health Infoway (infoway-inforoute.ca)

Canadian Association of Radiologists (2023) Artificial Intelligence Artificial Intelligence - CAR - Canadian Association of Radiologists

Health Canada (2023) Draft guidance document: Pre-market guidance for machine learning-enabled medical devices 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

Medicines and Healthcare products Regulatory Agency, UK (2023) Software and AI as a Medical Device Change Programme. https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme.

Vector Institute (2023) Health AI Implementation Toolkit https://vectorinstitute.ai/health-ai-implementation-toolkit/

The Canadian Law & HTA Working Group (2022) Legal Guidance for HTA Bodies (2022). https://drive.google.com/file/d/1nxsf4HRP9xYZaDi6oXmwB5YyberIbpHv/view

NHS (2021). The Digital Technology Assessment Criteria for Health and Social Care. https://transform.england.nhs.uk/key-tools-and-info/digital-technology-assessment-criteria-dtac/

Health Canada (2021) Good Machine Learning Practice for Medical Device Development: Guiding Principles https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/good-machine-learning-practice-medical-device-development.html

World Health Organization (2021) Ethics and governance of artificial intelligence for health https://www.who.int/publications/i/item/9789240029200

World Health Organization (2021) Generating Evidence for AI-Based Medical Devices https://iris.who.int/bitstream/handle/10665/349093/9789240038462-eng.pdf?sequence=1

Haute Autorité de Santé, France (2020) LPPR: Dossier submission to the Medical Device and Health Technology Evaluation Committee (CNEDiMTS) https://www.has-sante.fr/upload/docs/application/pdf/2020-10/guide_dm_vf_english_publi.pdf

Characteristics of Included Guidance

Table 1: Characteristics of Included Guidance

Guidance, Country	What is it? Who is the target audience?	Principal components addressed
Australian Government (2024) Artificial Intelligence (AI) and medical device software[1] Australia	Information for software manufacturers about how the Australian government regulates AI medical devices. Primary target: software manufacturers.	Clinical safety Usability and accessibility
Registered Nurses' Association of Ontario (2024) Clinical Practice in a Digital Health Environment[2] Canada	A best practice guideline on clinical practice in the digital health environment. In this guidance, the expert panel provides implementation tips for health care providers and organizations when implementing clinical decision support systems or early warning systems that use AI-driven predictive analytics. Primary target: nurses, members of the interprofessional team, educators and administrators	Clinical safety Usability and accessibility
Canada Health Infoway (2023) Digital Health Solutions Privacy and Security Guideline[3] Canada	This guideline outlines organizational recommendations and considerations to ensure the privacy and security of both patient health information and patient data and their lifecycle. A component of this guidance discusses health care AI. The guidance includes modules about the risks of AI in health care, emerging regulation of AI, identifying strategic opportunities and investments in AI, change management for AI adoption in the health care sector, and AI governance. Primary target: vendors, health care organizations, and patients.	Data protection Technical security
Canada Health Infoway (2023) Toolkit for Implementers of Artificial Intelligence in Health Care[4] Canada	A toolkit provides an overview of the issues related to implementing and using AI solutions in health care and offers strategic and operational guidance for designing responsible AI projects and governance programs. Primary target: Health care organizations at the early stages of considering or incorporating advanced technologies, such as AI into their operations.	Clinical safety Data protection Technical security Interoperability Usability and accessibility
Canadian Association of Radiologists (2023) Artificial Intelligence[5,6] Canada	A series of white papers from the Canadian Association of Radiologists on AI topics in radiology, including ethical and legal issues. Primary target: radiologists practicing in Canada.	Clinical safety Data protection Technical security Interoperability Usability and accessibility
Health Canada (2023) Draft guidance document: Pre-market guidance for machine learning-enabled medical devices[7] Canada	Pre-market guidance for ML system of an ML-enabled medical devices. It does not cover the non-ML information required in a medical device application. Primary target: manufacturer submitting a new or amendment application for Class II, III and IV MLMD under the regulations.	Clinical safety Data protection Technical security Usability and accessibility

Medicines and Healthcare products Regulatory Agency, UK (2023) Software and AI as a Medical Device Change Programme[8] UK	This guidance is aimed to ensure that medical device regulation is fit for purpose for software, including AI. Primary target: digital health innovators and adopters of these technologies.	Clinical safety Data protection Technical security Usability and accessibility
Vector Institute (2023) Health AI Implementation Toolkit[9] Canada	A toolkit developed to highlight common deployment barriers for those who are looking to implement innovative health AI research in a clinical context. This guidance includes a health AI implementation checklist. Primary target: individuals (e.g., researchers, clinicians, health professionals, others) who have developed a robust, mature health AI model or application and are looking to deploy their solution in a clinical environment.	Clinical safety Data protection Technical security Interoperability Usability and accessibility
The Canadian Law & HTA Working Group (2022) Legal Guidance for HTA Bodies[10] Canada	Guidance intended to support Canadian HTA bodies in incorporating legal analysis into their evaluations. Primary target: non-lawyers working within HTA bodies.	Clinical safety Data protection Usability and accessibility
NHS (2021) Digital Technology Assessment Criteria for health and social care UK	DTAC is the national baseline criteria for digital health technologies entering and already used in the NHS and social care. It contains assessment criteria for 5 core components: clinical safety, data protection, technical security, interoperability, and usability and accessibility. Primary target: developers and health care organizations who assess suppliers at the point of procurement or as part of a due diligence process.	Clinical safety Data protection Technical security Interoperability Usability and accessibility
Health Canada (2021) Good Machine Learning Practice for Medical Device Development: Guiding Principles[11] Canada	The U.S. Food and Drug Administration, Health Canada, and the UK's Medicines and Healthcare products Regulatory Agency jointly identified 10 guiding principles that can inform the development of Good Machine Learning Practice. These guiding principles will help promote safe, effective, and high-quality medical devices that use AI and ML. Primary target: manufacturer of medical devices that use AI and ML.	Clinical safety Data protection Technical security Usability and accessibility
World Health Organization (2021) Ethics and governance of artificial intelligence for health[12] International	This report endorses key ethical principles for the use of AI for health. Primary target: ministries of health	Clinical safety Usability and accessibility
World Health Organization (2021) Generating Evidence for AI-Based Medical Devices[13] International	A framework of considerations used in evaluating clinical evidence regarding AI-SaMD, aiming to help formulate a consensus for guiding validation, evidence generation and reporting across the total product life-cycle within a global health context. The guidance is divided into 3 sections: AI software development, AI software validations and reporting, and AI software deployment.	Clinical safety Usability and accessibility

	Primary target: policy makers with Ministries of Health, industry developers and researchers building AI tools, international users involved in the implementation of AI tools in global health, and for internal World Health Organization users.	
Haute Autorité de Santé, *France* (2020) LPPR: Dossier submission to the Medical Device and Health Technology Evaluation Committee (CNEDiMTS)[14] France	Guide for submitting an medical device and health technology for evaluative HTA assessment. Primary target: applicants (manufacturer, distributor, service provider).	Clinical safety Interoperability Usability and accessibility

AI = artificial intelligence; DTAC = Digital Technology Assessment Criteria for health and social care; HTA = health technology assessment; ML = mechine learning; MLMD = machine learning medical device; NHS = National Health Service; SaMD = software as a medical device.

Table 2: UK's Digital Technology Assessment Criteria, its Applicability to Health Care Context in Canada, and Artificial Intelligence Consideration Themes

Evidence Framework Domain	Code	Assessment Question	What is it and who is responsible in the UK?	Who is responsible in Canada?	Equivalent measure/strategy/policy in Canada? If yes, Describe
Section C1: Clinical Safety[a]	C1	Not applicable	Not applicable	Not applicable	Not applicable
	C1.1	Have you undertaken Clinical Risk Management activities for this product which comply with DCB0129?	The DCB0129 standard applies to organisations that are responsible for the development and maintenance of health IT systems. A health IT system is defined as "'product used to provide electronic information for health and social care purposes." Incident reporting for medical devices Federal (NHS)	Federal (Health Canada)	ISO 14971 applies to manufacturers of medical devices all over the world, including Canada.[15] List of recognized standards for medical devices.[16] Medical Devices Regulations (SOR/98-282) outlines safety and effectiveness requirements.[17] Software as a medical device (SaMD) Guidance, including risk classification of medical devices.[7,18] Guidance for incident reporting for medical devices, reporting a medical device problem (for health care professionals), and mandatory medical device problem reporting from industry (i.e., manufacturer, importer).[19-21] Mandated: yes
	C1.1.1	Please detail your clinical risk management system	DCB0129 sets out the activities that must and should be undertaken for health IT systems. An example clinical risk management system template can be downloaded from the NHS Digital website.	Federal (Health Canada)	Unclear; no equivalent template identified for medical devices. Mandated: yes

			Federal (NHS)		
	C1.1.2	Please supply your Clinical Safety Case Report and Hazard Log	Specifically, your DTAC submission should include: ● A summary of the product and its intended use ● A summary of clinical risk management activities ● A summary of hazards identified which you have been unable to mitigate to as low as it is reasonably practicable ● The clear identification of hazards which will require user or commissioner action to reach acceptable mitigation (for example, training and business process change) It should not include the hazard log in the body of the document - this should be supplied separately. Example Clinical Safety Case Report and Hazard Log templates can be downloaded from the NHS Digital website. Federal (NHS)	Federal (Health Canada)	Unclear; Health Canada provides guidance for incident reporting for medical devices, reporting a medical device problem (for health care professionals), and mandatory medical device problem reporting from industry (i.e., manufacturer, importer).[19-21]
	C1.2	Please provide the name of your Clinical Safety Officer (CSO), their profession and registration details	The CSO must: ● Be a suitably qualified and experienced clinician ● Hold a current registration with an appropriate professional body relevant to their training and experience ● Be knowledgeable in risk management and its application to clinical domains ● Be suitably trained and qualified in risk	Federal (Health Canada)	Unclear; Health Canada provides guidance for incident reporting for medical devices, reporting a medical device problem (for health care professionals),[21] and mandatory medical device problem reporting from industry (i.e., manufacturer, importer).[19-21]

			management or have an understanding in principles of risk and safety as applied to Health IT ● Have completed appropriate training The work of the CSO can be undertaken by an outsourced third party. Federal (NHS)		
	C1.3	If your product falls within the UK Medical Devices Regulations 2002, is it registered with the Medicines and Healthcare products Regulatory Agency (MHRA)?	If this question is not applicable because your product does not fall within the UK Medical Devices Regulations 2002, continue to question C1.4. If No, but the product falls within the UK Medical Devices Regulations 2002, continue to question C.1.3.2. The MHRA provides guidance on medical devices to place them on the market in Great Britain and Northern Ireland, regulatory requirements for all medical devices to be placed on the UK market, conformity assessment and the UK Conformity Assessed (UKCA) mark, classification of stand-alone medical device software (including apps) and how to tell if your product falls within the UK medical devices Regulations 2002. Federal (MHRA)	Federal (Health Canada)	Before manufacturers can sell a device in Canada, manufacturers of Class II, III and IV devices must obtain a medical device licence.[18] Although Class I devices do not require a licence, they are monitored through the establishment licensing process.[18] Class I: Medical Devices Establishment Licence Class II-V: Medical Devices Active Licence For medical devices in Canada, the application for a medical device license is completed through Health Canada.[22] The government of Canada and Health Canada provide guidance on regulatory requirements for medical devices[17] to be placed on the market in Canada, conformity assessment,[23] and classification of software as a medical device (including apps).[24] Health Canada also has an entire page devoted to compliance and

					enforcement of medical devices (e.g., forms, guidance, policies, laws).[25]
	C1.3.1	If yes, please provide your MHRA registration number	No further details provided. Federal (MHRA)	Federal (Health Canada)	Health Canada provides a license number.
	C1.3.2	If the UK Medical Device Regulations 2002 are applicable, please provide your Declaration of Conformity and, if applicable, certificate of conformity issued by a Notified Body / UK Approved Body	Medical device manufacturers must ensure that their device complies with the relevant Essential Requirements of the legislation and draw up a Declaration of Conformity to declare this. Class I devices with a measuring function and devices in Class IIa, IIb and III must undergo conformity assessment from an EU Notified Body or UK Approved Body which has been designated for medical devices, and be issued a certificate of conformity (commonly referred to as a "CE certificate" or "UKCA certificate"). Federal (MHRA)	Federal (Health Canada)	Health Canada's declaration of conformity.[23]
	C1.4	Do you use or connect to any third-party products?	If no, continue to section C2. DCB0129 contains the requirements in relation to third party products. Federal (NHS)	Unclear	Unclear: ISO 14971 may provide these details, but the document is behind a paywall.
	C1.4.1	If yes, please attach relevant Clinical Risk Management documentation and conformity certificate	No further details provided.	Not applicable	Not applicable
Section C2: Data Protection[b]	C2	Not applicable	Not applicable	Federal (Office of the Privacy Commissioner of Canada), Provincial (Office of the Information	**General overview of privacy laws in Canada**: PIPEDA (Personal Information Protection and Electronic Documents Act,

				and Privacy Commissioner of Alberta, Office of the Information & Privacy Commissioner for British Columbia, Commission d'accès à l'information du Québec)	S.C. 2000, c 5) generally applies to private-sector organizations that collect, use, and disclose personal health information (PHI) in the course of a commercial activity.[26] Alberta (Personal Information Protection Act, S.A. 2003, c.P-6.5), British Columbia (Personal Information Protection Act, SBC 2003, c.63, guide) and Quebec (An Act Respecting the Protection of Personal Information in the Private Sector, CQLR c P-39.1) have their own private-sector privacy laws that have been deemed substantially similar to PIPEDA.[4,27] "Organizations that are subject to a substantially similar provincial privacy law are generally exempt from PIPEDA with respect to the collection, use, or disclosure of personal information that occurs within that province."[26] "Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador have also adopted substantially similar legislation regarding the collection, use, and disclosure of PHI."[26] Collection, use, and disclosure of PHI by a physician would be governed by that jurisdiction's health privacy legislation, if one exists. Freedom of Information and Protection of Privacy and Health Information Acts are additional health privacy laws in Canada, which are governed at the provincial and territorial level.[4] Mandated: yes
	C2.1	If you are required to register with the	There are some instances where organisations are	Federal (Office of the Privacy Commissioner of	All businesses that handle personal are subject to privacy

		Information Commissioner, please attach evidence of a current registration. If you are not required to register, please attach a completed self-assessment showing the outcome from the Information Commissioner and your responses which support this determination.	not required to register with the Information Commissioner. This includes where no personal information is being processed. The Information Commissioner has a registration self-assessment tool to support this decision making. Federal (Information Commission's Office)	Canada), Provincial (Office of the Information and Privacy Commissioner of Alberta, Office of the Information & Privacy Commissioner for British Columbia, Commission d'accès à l'information du Québec)	laws (e.g., PIPEDA) but there does not appear to be a registration or data protection fee requirement.[26] PIPEDA (Voluntary) Self-Assessment Tool[28] Mandated: no
	C2.2	Do you have a nominated Data Protection Officer (DPO)?	Not all organisations are required to have a DPO. This is determined by the type of organisation and core activities. The most common reason for organisations providing digital health technologies to have a DPO is due to the core activities involving processing health data (being a special category). The Information Commissioner has a self-assessment tool to determine whether you must appoint a DPO. Federal (Information Commission's Office)	Federal (Office of the Privacy Commissioner of Canada), Provincial (Office of the Information and Privacy Commissioner of Alberta, Office of the Information & Privacy Commissioner for British Columbia, Commission d'accès à l'information du Québec)	Federal: PIPEDA Self-Assessment Tool describes the need to designate a privacy representative.[28] Provincial: British Columbia's act describes the requirement of designating 1 or more individuals are a privacy officer.[29] Alberta's 10 Steps to Implement Personal Information Protection Act (PIPA) states to put someone in charge and be the contact for the public and employees when privacy issues arise.[30] Quebec's Bill 64 states to designate a person in charge of the protection of person information.[31] Mandated: yes
	C2.2.1	If you are required to have a nominated DPO, please provide their name. If you are not	No further details provided.	Not applicable	Not applicable

		required to have a DPO please attach a completed self-assessment showing the outcome from the Information Commissioner and your responses which support this determination.			
	C2.3	Does your product have access to any personally identifiable data or NHS held patient data?	The UK General Data Protection Regulation (GDPR) applies to the processing of personal data. If no, continue to question C2.4 Federal (Information Commissioner's Office)	Provincial	Health Information Acts are additional health privacy laws in Canada, which are governed at the provincial and territorial level.[4] Mandated: yes
	C2.3 .1	Please confirm you are compliant (having standards met or exceeded status) with the annual Data Security and Protection Toolkit Assessment. If you have not completed the current year's assessment and the deadline has not yet passed, please confirm that you intend to complete this ahead of the deadline and that there are no material changes from your previous years submission that would affect your compliance.	The Data Security and Protection Toolkit allows organisations to measure performance against the National Data Guardian's 10 data security standards. Federal (NHS)	Provincial	Unclear; each province/territory would likely require/have their own toolkit given provincial/territorial legislation protects the confidentiality and privacy of PHI.

	C2.3.2	Please attach the Data Protection Impact Assessment (DPIA) relating to the product.	DPIA's are a key part of the accountability obligations under the UK GDPR, and when done properly help organisations assess and demonstrate how they comply with data protection obligations. The Information Commissioner has provided guidance on how to complete a DPIA and a sample DPIA template. Federal (Information Commissioner's Office)	Federal (for personal information guidance) and Provincial/Territorial (for health information guidance).	Examples of identified guidance: British Columbia's PIA guidance for the private sector[32] and associated template.[33] Mandated by Section 69 (5) of the Freedom of Information and Protection of Privacy Act. The province is also developing a Digital Privacy Impact Assessment (DPIA).[34] Alberta's guidance on PIA.[35] "Custodians are required to submit a PIA for review by the OIPC (section 64 of the Health Information Act). Public bodies and private sector organizations are not required to submit a PIA for review by the OIPC. The OIPC encourages public bodies and organizations to voluntarily submit PIAs."[35,36] Ontario's guidance for PIAs, and more recent guidance identified in the freedom of information and protection of privacy manual. Quebec mandates enterprises to conduct a PIA (p-39.1 - Act respecting the protection of personal information in the private sector). Mandated: jurisdiction dependent
	C2.4	Please confirm your risk assessments and mitigations / access controls / system level security policies have been signed-off by your DPO (if one is in place) or an accountable officer	No further details provided.	Not applicable	Not applicable

		where exempt in question C2.2.			
	C2.5	Please confirm where you store and process data (including any third-party products your product uses)	Individual organisations within the Health and Social Care system are accountable for the risk-based decisions that they must take. Federal	Not applicable	Not applicable
	C2.5.1	If you process store or process data outside of the UK, please name the country and set out how the arrangements are compliant with current legislation	From 1 January 2021, the UK GDPR applies in the UK in place of the "EU GDPR'. The UK GDPR will carry across much of the existing EU GDPR legislation. The Department for Digital, Culture, Media & Sport has published two Keeling Schedules which show the changes to the Data Protection Act 2019 and EU GDPR. The Information Commissioner has published guidance on international data transfers after the UK exit from the EU Implementation Period. Federal (Information Commissioner's Office)	Federal (Office of the Commissioner of Canada)	Guidance for how PIPEDA applies to processing personal data across borders.[37] Mandated: yes
Section C3: Technical Security[c]	C3	Not applicable	Not applicable	Not applicable	Not applicable
	C3.1	Please attach your Cyber Essentials Certificate	Cyber Essentials helps organisations guard against the most common cyber threats. The National Cyber Security Centre (NCSC) have published cyber security guidance for small	Federal Dept/Agency: • Innovation, Science and Economic Development Canada	CyberSecure Canada from Innovation, Science and Economic Development Canada is a Federal cyber certification program that aims to raise the cyber security baseline among Canadian SMEs, increase consumer confidence in the

			to medium enterprises (SME's). Federal (NCSC)	• Communications Security Establishment Canada • Health Canada	digital economy, promote international standardization and better position SMEs to compete globally.[38] To be eligible for certification the organization must implement the security controls in the National Standard CAN/CIOSC 104:2021 Baseline cyber security controls for small and medium organizations (Digital Governance Council, not for profit organization).[39] Canadian Centre for Cyber Security from Communications Security Establishment Canada has published updated cyber security guidance for SMEs.[40] Mandated: yes
	C3.2	Please provide the summary report of an external penetration test of the product that included Open Web Application Security Project (OWASP) Top 10 vulnerabilities from within the previous 12-month period.	The NCSC provides guidance on penetration testing. The OWASP Foundation provides guidance on the OWASP top 10 vulnerabilities. Federal (NCSC)	Federal Dept/Agency: • Health Canada • Communications Security Establishment Canada	Health Canada published a guidance document outlining pre-market requirements for medical device cyber security, which mentions structured penetration testing.[15] Canadian Centre for Cyber Security from Communications Security Establishment Canada provides guidance on the top measures to enhance cyber security for SMEs (ITSAP.10.035; brief guidance provided for penetration testing of websites).[41,42] The OWASP Foundation is a not-for-profit organization that has educational resources, guidelines, and open-source tools to help improve the security of the software SMEs use. They provide guidance on the OWASP

					top 10 vulnerabilities,[43] and penetration testing methodologies.[44] Mandated: yes
	C3.3	Please confirm whether all custom code had a security review.	The NCSC provides guidance on producing clean and maintainable code.[45] Federal (NCSC)	Federal (e.g., Health Canada)	Health Canada provides guidance document about pre-market requirements for medical device cyber security), including different types of testing (e.g. known vulnerability testing, malware testing). [15]The NCSC does provide more details on how to producing clean and maintable code.[45]
	C3.4	Please confirm whether all privileged accounts have appropriate Multi-Factor Authentication (MFA)?	The NCSC provides guidance on Multi-Factor Authentication. Federal (NCSC)	Federal (Communications Security Establishment Canada)	Canadian Centre for Cyber Security from Communications Security Establishment Canada provides guidance on MFA for organizations and individuals, and also highlights enforcing strong user identification (e.g., MFA) as a top measure to enhance cyber security for small and medium organizations.[42] Mandated: no, recommended.
	C3.5	Please confirm whether logging and reporting requirements have been clearly defined.	The NCSC provides guidance on logging and protective monitoring. To confirm yes to this question, logging (e.g., audit trails of all access) must be in place. It is acknowledged that not all developers will have advanced audit capabilities. Federal (NCSC)	Federal (Communications Security Establishment Canada)	Canadian Centre for Cyber Security from Communications Security Establishment Canada provides about network security logging and monitoring (ITSAP.80.085), including a checklist of network security logging and monitoring best practices.[46] Mandated: no, recommended.
	C3.6	Please confirm whether the product has been load tested	Load testing should be performed. Federal	Unclear, likely Federal	Unclear

Section C4: Interoperability criteria[d]	C4	Not applicable	Not applicable	Not applicable	Not applicable
	C4.1	Does your product expose any Application Programme Interfaces (API) or integration channels for other consumers?	The NHS website developer portal provides guidance on APIs and the NHS. Government Digital Services provide guidance on Open API best practice. Federal (NHS, Government Digital Services)	Federal (e.g., Treasury Board of Canada Secretariat and broadly through the Government of Canada's website), Provincial (e.g., Ontario Health)	The government of Canada provides API Guidance.[47] The Treasury Board of Canada Secretariat provides Government Standards on APIs[48] Digital health information exchange (DHIEX) is the regulatory framework.[49] that gives Ontario Health the ability to define and implement the health information standards and requirements for use in interoperability specifications. It is unclear if other provinces or territories have similar frameworks. In addition, Canada Health Infoway has been responsible for licensing, defining and maintaining pan-Canadian standards that promote interoperability.[50] Mandated: yes
	C4.1.1	If yes, please provide detail and evidence: ● The API's (e.g., what they connect to) set out the health care standards of data interoperability e.g., Health Level Seven International (HL7) / Fast Healthcare Interoperability Resources (FHIR) ● Confirm that they follow Government Digital Services	same as above (C4.1)	Not applicable	Not applicable

		Open API Best Practice ● Confirm they are documented and freely available ● Third parties have reasonable access to connect If no, please set out why your product does not have APIs.			
	C4.2	Do you use NHS number to identify patient record data?	NHS Digital provides guidance on NHS Login for partners and developers. Federal (NHS)	Not applicable to Canada with its current health care structure.[51]	Not applicable
	C4.2.1	If yes, please confirm whether it uses NHS Login to establish a user's verified NHS number. If no, please set out the rationale, how your product established NHS number and the associated security measures in place.	Same as above (C4.2)	Not applicable	Not applicable
	C4.3	Does your product have the capability for read/write operations with electronic health records (EHRs) using industry standards for secure interoperability (e.g. OAuth 2.0, TLS 1.2)	No further details provided. Industry standard	Unclear, OAuth 2.0 is an industry standard, but Canada's current health care structure doesn't have EMRs managed at the federal level.[51]	The government of Canada's website provides API security best practices[52] and describes industry standards for secure interoperability (e.g., OAuth 2.0,[53] among others). Mandated: yes
	C4.3.1	If yes, please detail the standard	Same as above (C4.3)	Not applicable	Not applicable
	C4.3.2	If no, please state the reasons and mitigations,	Same as above (C4.3)	Not applicable	Not applicable

		methodology and security measures.			
	C4.4	Is your product a wearable or device, or does it integrate with them?	If no, continue to section D.	Not applicable	Not applicable
	C4.4.1	If yes, provide evidence of how it complies with ISO/IEEE 11073 Personal Health Data (PHD) Standards.	Access the ISO Standard. This is a paid-for document. Note. This example ISO has been withdrawn. The new ISO is found here: ISO 41064:2023 - Health informatics — Standard communication protocol — Computer-assisted electrocardiography International Organization for Standardization is an industry standard.	International Organization for Standardization is an industry standard.	International standard would apply in Canada: ISO/IEE 10073.[54] Mandated: yes
Section D1: Usability and accessibility[e]	**D**	Not applicable	Not applicable		Unclear; Government of Canada Digital Standards: Design Ethical Services and Empower staff to deliver better services[55f]
	D1.1	**Understand users and their needs in context of health and social care** Do you engage users in the development of the product?	NHS Service Standard Point 1 Federal (NHS)	Federal (Treasury Board of Canada Secretariat)	Unclear; Government of Canada Digital Standards: Design with Users[55f]
	D1.1.1	If yes or working towards it, how frequently do you consider user needs in your product development and what methods do you use to engage users and	Same as above (D1.1)	Not applicable	Not applicable

		understand their needs?			
	D1.2	**Work towards solving a whole problem for users** Are all key user journeys mapped to ensure that the whole user problem is solved, or it is clear to users how it fits into their pathway or journey?	NHS Service Standard Point 2 and Point 3 are often dealt with by teams together. Federal (NHS)	Federal (Treasury Board of Canada Secretariat)	Unclear; Government of Canada Digital Standards: Collaborate Widely and Design with Users[55f]
	D1.2.1	If yes or working towards it, please attach the user journeys and/or how the product fits into a user pathway or journey	same as above (D1.2)	Not applicable	Not applicable
	D1.3	**Make the service simple to use** Do you undertake user acceptance testing to validate usability of the system?	NHS Service Standard Point 4 Federal (NHS)	Federal (Treasury Board of Canada Secretariat)	Unclear; Government of Canada Digital Standards: Design with Users[55f]
	D1.3.1	If yes or working towards it, please attach information that demonstrates that user acceptance testing is in place to validate usability.	same as above (D1.3)	Not applicable	Not applicable
	D1.4	**Make sure everyone can use the service** Are you international Web Content Accessibility Guidelines (WCAG)	NHS Service Standard Point 5 The Service Manual provides information on WCAG 2.1 level AA. The Government Digital Service provides guidance	Federal (Treasury Board of Canada Secretariat)	Unclear; Government of Canada Digital Standards: Build in Accessibility from the Start[55 f] WCAG is utilized in Canada.[56] The Treasury Board of Canada Secretariat is currently reviewing the Standard on Web

		2.1 level AA compliant?	on accessibility and accessibility statements, including a sample template. Federal (NHS)		Accessibility. However, as part of a commitment to an accessible and barrier-free Canada, it is recommended that organizations adopt the Harmonized European Standard (EN 301 549) (English only) and adhere to guidance available in the Guideline on Making Information Technology Usable by All.[56]
	D1.4.1	Provide a link to your published accessibility statement.	same as above (D1.4)	Not applicable	Not applicable
	D1.5	**Create a team that includes multi-disciplinary skills and perspectives** Does your team contain multidisciplinary skills?	NHS Service Standard Point 6 Federal (NHS)	Federal (Treasury Board of Canada Secretariat)	Unclear; Government of Canada Digital Standards: Collaborate Widely[55 f]
	D1.6	**Use agile ways of working** Do you use agile ways of working to deliver your product?	NHS Service Standard Point 7 Federal (NHS)	Federal (Treasury Board of Canada Secretariat)	Unclear; Government of Canada Digital Standards: Iterate and Improve Frequently and Be Good Data Stewards[55 f]
	D1.7	**Iterate and improve frequently** Do you continuously develop your product?	NHS Service Standard Point 8 Federal (NHS)	Federal (Treasury Board of Canada Secretariat)	Unclear; Government of Canada Digital Standards: Iterate and Improve Frequently and Be Good Data Stewards[55 f]
	D1.8	**Define what success looks like and be open about how your service is performing** Do you have a benefits case that includes your	NHS Service Standard Point 10 Federal (NHS)	Federal (Treasury Board of Canada Secretariat)	Unclear; Government of Canada Digital Standards: Work in the Open by Default and Be Good Data Stewards[55f]

		objectives and the benefits you will be measuring and have metrics that you are tracking?			
	D1.9	**Choose the right tools and technology** Does this product meet with NHS Cloud First Strategy?	NHS Service Standard Point 11 NHS Internet First Policy [**program is now closed**]. Federal (NHS)	Federal (Treasury Board of Canada Secretariat)	Unclear; Government of Canada Digital Standards: Build in Accessibility from the Start[55f] The UK guidance is more complete for some aspects, but there are certain components of NHS Service Standard Point 11 that also align with Section C4, interoperability of DTAC and some AI considerations related to technical infrastructure and integration and sustainability.
	D1.9.1	Does this product meet the NHS Internet First Policy?	same as above (D1.9)	Not applicable	Not applicable
	D1.10	**Use and contribute to open standards, common components and patterns** Are common components and patterns in use?	NHS Service Standard Point 13 Federal (NHS)	Federal (Treasury Board of Canada Secretariat)	Unclear; Government of Canada Digital Standards: Use Open Standards and Solutions[55f]
	D1.10.1	If yes, which common components and patterns have been used?	same as above (D1.10)	Not applicable	Not applicable
	D1.11	**Operate a reliable service** Do you provide a Service Level Agreement to all customers purchasing the product?	NHS Service Standard Point 14 Federal (NHS)	Federal (Treasury Board of Canada Secretariat)	Unclear; Government of Canada Digital Standards: Design with Users and Build Accessibility from the start.[55f] The UK guidance is more complete for some aspects, but there are certain components of NHS Service Standard Point 14 that also align with AI considerations related to

					monitoring, maintenance, and sustainability.
	D1.12	Do you report to customers on your performance with respect to support, system performance (response times) and availability (uptime) at a frequency required by your customers?	same as above (D1.11)	Not applicable	Not applicable
	D1.12.1	Please attach a copy of the information provided to customers	same as above (D1.11)	Not applicable	Not applicable
	D1.12.2	Please provide your average service availability for the past 12 months, as a percentage to two decimal places	same as above (D1.11)	Not applicable	Not applicable

API = Application Programme Interfaces; AI = artificial intelligence; CSO = Clinicial Safety Officer; Dept = department; DHIEX = Digital health information exchange; DPIA = Data Protection Impact Assessment; DPO = Data Protection Officer; DTAC = Digital Technology Assessment Criteria; EU = European Union; GDPR = General Data Protection Regulation; ISO = International Organization for Standardization; MFA = Multi-Factor Authentication; MHRA = Medicines and Healthcare products Regulatory Agency; NCSC = National Cyber Security Centre; NHS = National Health Service; OIPC = Office of the Information and Privacy Commissioner; OWASP = Open Worldwide Application Security Project; PHI = Personal Health Information; PIA = Privacy Impact Assessment; PIPA = Personal Information Protection Act; PIPEDA = Personal Information Protection and Electronic Documents Act; SaMD = Software as a Medical Device; SMEs = small and medium-sized enterprises; WCAG = Web Content Accessibility Guidelines.

[a] **C1 – Clinical safety description from DTAC**: "Establishing that your product is clinically safe to use. You must provide responses and documentation relating to the specific technology product that is subject to assessment. The DCB0129 standard applies to organisations that are responsible for the development and maintenance of health IT systems. A health IT system is defined as "product used to provide electronic information for health and social care purposes". DTAC is designed as the assessment criteria for digital health technologies and C1 Clinical Safety Criteria is intended to be applied to all assessments. If a developer considers that the C1 Clinical Safety is not applicable to the product being assessed, rationale must be submitted exceptionally detailing why DCB0129 does not apply. The DCB0160 standard applies to the organisation in which the health IT is deployed or used. It is a requirement of the standard (2.5.1) that in the procurement of health IT systems the organisation must ensure that the manufacturer and health IT system complies with DCB0129. The organisation must do so in accordance with the requirements and obligations set out in the DCB0160 standard. This includes personnel having the knowledge, experience and competences appropriate to undertaking the clinical risk management tasks assigned to them and organisations should ensure that this is the case when assessing this section of the DTAC. If the CSO or any other individual has concerns relating to safety of a medical device including software and apps, this should be reported to the MHRA) using the Yellow Card reporting system: Report a problem with a medicine or medical device - GOV.UK (www.gov.uk)."

[b] **C2 – Data protection description from DTAC**: "Establishing that your product collects, stores and uses data (including personally identifiable data) compliantly. This section applies to the majority of digital health technology products however there may be some products that do not process any NHS held patient data or any identifiable data. If this is the case, the DPO, or other suitably authorised individual should authorise this data protection section being omitted from the assessment."

[c] **C3 – Technical security description from DTAC**: "Establishing that your product meets industry best practice security standards and that the product is stable. Dependent on the digital health technology being procured, it is recommended that appropriate contractual arrangements are put in place for problem identification and resolution, incident management and response planning and disaster recovery. Please provide details relating to the specific technology and not generally to your organisation."

[d] **C4 – Interoperability criteria description from DTAC**: "Establishing how well your product exchanges data with other systems. To provide a seamless care journey, it is important that relevant technologies in the health and social care system are interoperable, in terms of hardware, software and the data contained within. For example, it is important that data from a patient's ambulatory blood glucose monitor can be downloaded onto an appropriate clinical system without being restricted to one type. Those technologies that need to interface within clinical record systems must also be interoperable. APIs should follow the Government Digital Services Open API Best Practices, be documented and freely available and third parties should have reasonable access in order to integrate technologies. Good interoperability reduces expenditure, complexity and delivery times on local system integration projects by standardising technology and interface specifications and simplifying integration. It allows it to be replicated and scaled up and opens the market for innovation by defining the standards to develop upfront. This section should be tailored to the specific use case of the product and the needs of the buyer however it should reflect the standards used within the NHS and social care and direction of travel. Please provide details relating to the specific technology and not generally to your organisation."

[e] **D1 – Usability and accessibility description from DTAC**: "Establishing that your product has followed best practice. Please note that not all sections of the NHS Service Standard are included where they are assessed elsewhere within DTAC, for example clinical safety."

[f] The Government of Canada Digital Standards[55] intend to improve government services in the digital age and are targeted for government practice (i.e., not directed to industry or consumer products specifically). However, the content, headings, and descriptions provided in these standards largely overlap with the NHS Service Standards,[57] as denoted in the table. The Government of Canada Digital Standards were the closest equivalent identified for the health care context in Canada, and it is unclear if there are other service standards in place for industry/consumer products.

Table 3: Examples of Implementation Considerations Identified for Artificial Intelligence-Enabled Medical Devices

Evidence Framework Domain	AI consideration themes	Implementation considerations identified for AI-enabled medical devices

Section C1: Clinical Safety	Monitoring, maintenance, and sustainability throughout the AI product lifecycle.	<u>Monitoring, maintenance, and sustainability throughout the AI product lifecycle.</u>
		• "Promote human well-being human safety and the public interest AI technologies should not harm people. They should satisfy regulatory requirements for safety, accuracy and efficacy before deployment, and measures should be in place to ensure quality control and quality improvement."[12]
		• Performance and validation.
		  ○ Health Canada's draft guidance reiterates the need for manufacturers of MLMDs to provide performance/bench testing or software verification and validation information (e.g., "descriptions of the chosen performance metrics, acceptance criteria and operating point/threshold with clinical and risk-based justifications; evidence to demonstrate that the ML system performs as intended and meets expected performance requirements when integrated as part of the medical device system or software; evidence to support the performance of the ML system for appropriate subgroups", such as underrepresented populations, and robustness training). "Manufacturers should also provide the appropriate clinical evidence, including clinical validation studies, to support the safe and effective clinical use of their device."[7]
		  ○ "Have you completed a silent trial prior to integration?"[9] An important step before AI model integration to ensure that the model is reliable and effective. "A silent trial in clinical AI deployment is a phase where the AI system's predictions or assessments are made and recorded but not yet used or visible to the practitioners, allowing the evaluation of its performance and accuracy in a real-world setting without impacting patient care. The silent trial bridges initial model development and clinical deployment and evaluation to evaluate the safety, reliability, and feasibility of the AI model in a minimal risk environment."[9]
		  ○ "What are the results of the model validation (key performance indicators) against test data?"[9] The following ensures the "model validation process is comprehensive and rigorous, and the model is robust and generalized well to new and unseen data. This will ultimately lead to improved outcomes while maximizing patient safety and privacy." The Vector Institute also lists the following considerations: Evaluate the performance of the model on the test data using multiple key performance indicators, conduct a sensitivity analysis to determine the impact of different thresholds and parameters on the model's performance, evaluate the model's performance on subgroups of the population to determine whether the model is biased towards certain groups, compare the performance of the model to that of other models or standard clinical practice to determine whether the model provides added value, and assess the impact of the model's performance to ensure that it aligns with the intended clinical application.[9]
		  ○ "What are the metrics used to evaluate model performance, and how are they aligned with the proposed use case?"[9] The Vector Institute provides the related

prompts to consider: “What is the intended clinical application for the AI model? Have you ensured that the labeled data used in training the AI model match the Gold Standard in clinical practice?” “What performance metrics have been chosen for the model, and why? How have the chosen metrics been validated by end users to ensure that they are appropriate for the proposed use case?” What are the end users’ thresholds for acceptance? What is the impact of having false positives and false negatives? For which metric(s) should you optimize in your use case? Have you conducted a clinical validation study to evaluate the performance of the model on real-world data? If so, what were the results?”[9]

- “Post-market surveillance and monitoring regularly generates new data such as safety reports, results from published literature, registries, post-market clinical follow-up studies, and other data about the use of AI-SaMD. This data needs to be checked for information that has the potential to change the evaluation of the risk/benefit analysis, and the clinical performance and clinical safety of the device.”[13]
- “In view of the character of AI systems, it is important that the regulatory system enables continuous modifications for improvement to be made throughout the AI system’s development lifecycle. The term “change” refers to such modifications, including those performed during maintenance. There are several proposed change management models and approaches for AI-based systems. Some consider change as part of the total development lifecycle and others focus on the change management process in the total lifecycle of medical device products which can be continuously improved.”[58]
- “Deployed Models Are Monitored for Performance and Re-training Risks are Managed: Deployed models have the capability to be monitored in “real world” use with a focus on maintained or improved safety and performance. Additionally, when models are periodically or continually trained after deployment, there are appropriate controls in place to manage risks of overfitting, unintended bias, or degradation of the model (for example, dataset drift) that may impact the safety and performance of the model as it is used by the Human-AI team.”[11]
- “Increased pre-market review and continuous post-approval surveillance are needed to strengthen the regulation of AI in or as medical devices.”[10] This is with the understanding that “many AI tools, especially ML that digests information in real-time as part of its learning.”[10]
- Include a “description of the processes, surveillance plans and risk mitigations in place to ensure ongoing performance and inter-compatibility of the ML system.”[7]
- “Do you have a plan on how to maintain and update the model after deployment?’[9] “Maintaining and updating an AI model requires ongoing attention and effort, but it is essential to ensure that the model continues to deliver value to the organization over time. By following these steps, you can help ensure that your AI model remains accurate, reliable, and effective in meeting the needs of your organization.” “Maintaining and updating an AI model after deployment is critical to ensure that the model continues to perform well, impacts patient care positively, and delivers value to the organization.”[9] “Monitor the model’s performance regularly to ensure that it is still delivering accurate and reliable results” (e.g.,

automated monitoring, manual monitoring). In addition, the Vector institute lists the following considerations: collect new data on an ongoing basis to help improve the model's performance, re-evaluate the model periodically to determine it still meets the needs of the organization, update the model as needed if any concerns arise, test the updated model thoroughly to ensure it is working as intended, deploy an updated model into production once it is thoroughly tests and validated, and monitor the updated model to ensure it's still delivering accurate and reliable results.[9]

- "How will you monitor model performance?Monitoring the performance of an AI model is essential to ensure that it continues to perform effectively and safely in a clinical setting" [9] The Vector institute lists the following ways to monitor the performance of an AI model in a clinical setting:
  - defining metrics (i.e., relevant to the clinical use case and aligned with the objectives of the model), establishing monitoring
  - establish monitoring procedures: designed to provide timely and relevant information about the model's performance in a clinical setting, e.g., real-time monitoring
  - collect relevant and accurate data on an ongoing basis to ensure a model's performance can be tracked over time.
  - analyze data to evaluate model's performance
  - take action to address any concerns related to the model's performance [9]
- Registered Nurses' Association of Ontario's best practice guideline emphasizes monitor the unintended impacts of implementing an AI tool regularly in addition to evaluating clinical outcomes; and "monitor and evaluate staff adherence to using the system and relevant clinical outcomes following implementation."[2]
- Human-AI team performance. "Focus Is Placed on the Performance of the Human-AI Team: Where the model has a "human in the loop," human factors considerations and the human interpretability of the model outputs are addressed with emphasis on the performance of the Human-AI team, rather than just the performance of the model in isolation."[11]

- Risk assessment and management.
  - Provide evidence of risk management to address risks (e.g., performance degradation such as data drift).[1,7,11]
  - The Vector Institute provides examples of risk assessment of harms: "If the system does not operate as intended, could it negatively impact patients' standard of care? Could the AI system result in harm or damage to the physical, or psychological well-being of individuals or society? Could the output from the AI system result in denying services for a patient? Could the output from the AI system result in discriminatory or biased outcomes? What is the likelihood of harm from an error in system output? What is the severity of harm from an error in system output?"[4]
  - The Vector Institute provides example questions for AI vendor assessment regarding risk management: "Does the vendor have a documented risk management process about the operation of their AI system" (e.g., vendor

identified known and possible risks of using their computer system)? What controls has the vendor put in place to reduce the risk of harm? "Is the vendor prepared to be part of your organization's risk assessment protocol?" "Has the vendor performed an AI liability assessment?"[4]
    - The Canadian Law & HTA Working Group presents considerations for HTA bodies to ask sponsors: "is this unlocked or locked ML as part of a medical device? What risk classification was provided to Health Canada and were there any terms/conditions as part of the licence provided? Is the manufacturer or sponsor aware of any complaints or concerns raised whether in Canada or internationally about the safety of the device?"[10]
    - WHO recognizes the "inherent incremental software changes could impact safety performance of AI-SaMDs" and emphasizes a "need for rigorous AI software version management and post-deployment surveillance to ensure that safety and performance metrics are maintained over time."[13] "Given the likelihood of AI-SaMD version updates, it is worth noting that incremental software changes – whether continuous or iterative, intentional or unintentional – could have serious consequences on safety performance after deployment. It is therefore vitally important that such changes are documented and identified by software version, and that a robust post-deployment surveillance plan is in place."[13]
    - Health Canada's draft guidance states manufacturers should conduct the necessary risk management by considering the following items in the risk analysis: erroneous outputs (e.g., false positive or false negative results, incorrect information for use in diagnosis or treatment); bias (e.g., a sex and gender-based analysis plus analysis may address some sources of unwanted bias); outfitting (e.g., an issue that occurs when a model is fit to properties that are specific to the training examples, resulting in a model that doesn't apply to the general problem it's intending to address); underfitting (when a model is not fit to all relevant properties of the population from the training examples, resulting in a model that does not apply to the general problem its meant to address); degradation of ML system performance (can occur from shifts in population demographics or disease incidence, changes in clinical practice, changes in clinical disease presentation, changes in input format or quality); automation bias (when a user's conclusion is overly reliant on the device output while ignoring contrary data or conflicting human decisions); alarm fatigue (an issue that occurs when a user is desensitized to alarms due to excessive exposure, which can result in missed alarms); risks associated with using a PCCP; and impacts of a PCCP on risk management. Many of these examples are also described in other guidance.[1,7,11]
- Data quality testing. Vector Institute suggests implementing "processes to regularly check, clean, and improve your data quality to ensure its accuracy and consistency."[9]
    - Example questions from Canada Health Infoway for AI vendor assessment and/or risk assessment for an organization regarding data quality testing: "Does the vendor have documented processes to test data for completeness, representativeness, and accuracy?" "Has an assessment been done to see if the source of data is suitable for the intended purpose (including how and why the data was collected)? Has the vendor identified any potential data gaps or

		shortcomings, and how those gaps and shortcomings can be addressed? Has the dataset been examined with a view toward potential bias? This includes ensuring that it is representative of the population to which the algorithm will be applied. Has the data been adequately prepared (e.g., through clear annotations, labeling and aggregations)? What are the key performance indicators and minimum performance metrics that the system must meet, as determined by the vendor? Has the vendor put in place a regular audit process to evaluate the ongoing use of its system?"[4] • Sustainability. "Continuous improvement and innovation. AI system should incorporate feedback and continuously improve based on user needs and technological advancements to keep the system relevant and beneficial in the longer term."[9] "Implement monitoring and alerts to detect and address any issues with the data pipeline in a timely manner."[9] ○ Promote AI that is responsive and sustainable. "Responsiveness requires that designers, developers and users continuously, systematically and transparently examine an AI technology to determine whether it is responding adequately, appropriately and according to communicated expectations and requirements in the context in which it is used." "Responsiveness also requires that AI technologies be consistent with wider efforts to promote health systems and environmental and workplace sustainability."[12] ○ The Vector Institute provides example components of the sustainability strategy of the AI tool related to clinical safety: ▪ "Continuous clinical validation of the AI system is necessary to ensure its accuracy, efficacy, and safety."[9] ▪ "Performance monitoring: regularly monitoring the system's performance and impact on patient outcomes" to "identify any issues that need to be addressed and demonstrate the value of the system to stakeholders [users]."[9] ▪ "maintenance and support: regular updates, bug fixes, and technical are necessary to ensure the system continues to operate effectively and reliably".[9]
Section C2: Data Protection	AI data governance and data protection. Multi-disciplinary, data governance team throughout the AI product lifecycle. Monitoring, maintenance, and sustainability.	<u>AI data governance and data protection.</u> • Vector Institute,[9] Health Canada,[11] and Canada Health Infoway[3] suggest establishing organizational policies and procedures that cover all aspects needed for AI data governance, such as data quality management, data privacy and security, data access and sharing, data lifecycle management, and regulatory compliance. They also emphasize responsible use and deployment of AI defining standards for data collection, storage, and use related to AI deployment (e.g., adopting standardized data models or terminologies, defining standard procedures for data entry and coding).[3,9,11] • Data governance has to be progressive, enabling access to the right data for the right people at the right time.[3,9] Different data types may require different handling and policies (e.g., clinical data, demographic data, financial data). • Canada Health Infoway emphasizes conducting a Privacy Impact Assessment and Threat and Risk Assessment on an applicable health care system that uses AI.[3] • Canada Health Infoway provides AI training and operationalization considerations including consent, de-identifying data, complying with individual rights under privacy laws, safely

transmitting the data, and inconsistent privacy laws. “Emerging legislation advocates for robust de-identification methodologies and caution against the risk of re-identification.”[4]

- De-identification and Re-identification. “Large representative data sets based on de-identified personal health information are important to create safe AI and to minimize the potential risk of algorithmic bias. However, there is a risk that the data may be re-identified.” There are various provincial privacy laws providing penalties for those who deliberately re-identify data (e.g., Quebec and Ontario’s privacy laws).[10]
- Canadian Association of Radiologists also highlights the “ownership of electronic medical records and the secondary use of de-identified medical data is a complex issue that will likely depend on the type of use.” Canadian Association of Radiologists states “tools and policies are required to facilitate and standardize anonymization of medical images”, which is likely relevant for other specialties as well. Canadian Association of Radiologists also highlights “public education campaigns should inform the public of the benefits that sharing of fully anonymized personal health data can provide.”[6]
- Vector Institute reiterates the importance of robust data management and privacy protections and law compliance, given the nature of sensitive health data. They suggest establishing “guidelines for ethical decision-making regarding the data collection, use, and sharing.”[9]
- Canada Health Infoway suggests implementors of an AI system should create a code of ethics and principles for AI, provide ethics training, and establish an ethics board or sub-committee. Examples of policies and procedures: principles of AI ethics, codes of conduct, AI ethics curricula.[4]
- “How have you ensured that patient data is being used ethically and in compliance with data protection laws?”[9]
- Protect autonomy. “The principle of autonomy requires that any extension of machine autonomy not undermine human autonomy. In the context of health care, this means that humans should remain in full control of health-care systems and medical decisions. Related duties to protect privacy and confidentiality and to ensure informed, valid consent by adopting appropriate legal frameworks for data protection.”[12]
    - Data governance in Canada requires considering and respecting First Nations, Inuit, and Métis data sovereignty principles (e.g., the First Nations principles of OCAP®,[59] Manitoba Métis principles of OCAS,[60] and Inuit Qaujimajatuqangit[61]), which have implications for guiding the respectful governance of data collected with, from, or about Indigenous peoples.
    - “Track or manage human reliance on the model by establishing a plan to review predictions. This will help mitigate automation bias and allow an objective standpoint on the model’s performance.”[9]
    - The Canadian Association of Radiologists also highlights “respect of data privacy requires balancing of principles of beneficence and justice (to improve medical care for others via secondary use of an individual's data) versus autonomy (as regards the concept of free and ongoing informed consent). Historically, institutional review boards have granted waivers of consent when gaining explicit consent is impractical, risk associated with data sharing is minimal, and data custodian is trusted.[6] To facilitate development of AI applications in health care, a

transition from “informed consent” for specific data uses, to “broad consent,” “opt-out consent,” and/or “presumed consent” to more general data uses is required.”[6]
    - “Recourse. Users should have recourse options made available to challenge any decision made about them by an automated decision-making systems.”[4] “When appropriate, consider how individuals can opt out of being included in the data used to train or run the AI system.”[4]
    - Disclosure and Notices. “Individuals should be given notice that a decision will be made in whole or in part by an automated decision-making system. Upon request, an organization should make available a general account of how it makes use of automated decision-making systems that could impact an individual personally. A designated human point of contact should be made available for individuals that may want more information or to contest a decision or output made by the system.”[4]
    - General risk assessment questions regarding law impacts reiterated by Canada Health Infoway: “What laws and regulations apply to this AI system, and are there any compliance requirements that must be met and documented? Are there specific compliance requirements that need to be met and documented? Has a legal assessment been conducted to identify liabilities and other legal issues?”[4]
- Further example questions from Canada Health Infoway for AI vendor assessment regarding commitment to responsible innovation, data access and data sharing: “Does the vendor have a track record of providing reputable services and a demonstrated commitment to responsible and ethical innovation? Can the vendor demonstrate examples of how it addresses ethical practices when delivering AI? Does the vendor have ethical frameworks or specific AI policies in place?” “Will the vendor allow your organization to access the data used and produced by the system? If restricted access is justified, will the vendor provide representative sampled data sets? Will your organization be providing any data to the vendor? If so, what data governance standards and policies does the vendor have in place? Will your organization provide any data that could contain personal or sensitive information? What mechanisms will be used to protect the security of the data in transit?”[4]

<u>Multi-disciplinary, data governance team throughout the product life cycle.</u>

- Enhance your data governance team by including members from diverse areas such as privacy, security, information technology, legal clinical, and executive staff.[9] Canada Health Infoway also highlights clinical and subject matter experts along with data scientists, data engineers, product manager, ethicists, lawyers, senior management, human resources, and vendors.[4]
- “multi-disciplinary expertise is leveraged throughout the total product life cycle: In-depth understanding of a model’s intended integration into clinical workflow, and the desired benefits and associated patient risks, can help ensure that MLMDs are safe and effective and address clinically meaningful needs over the lifecycle of the device.”[11]
- “Is it clearly understood who is responsible for the safe and continuous maintenance, operation, re-training, and decommissioning of the system?”[4]
- Example of a question from Canada Health Infoway for AI vendor assessment: “Does the vendor have a diverse, multidisciplinary team?”[4]

<u>Monitoring, maintenance, and sustainability.</u>

		• "Monitor whether new privacy and security requirements are put in place for health care AI." "Develop a security control profile to monitor and mitigate the identified risks to privacy and security based on assessment result. Track the AI technological disruption being presented by including threats to privacy and security. Maintain a process for assessing risks of re-identification." "De-identification or anonymization of patient health data may be compromised or even rendered ineffective in light of new algorithms that effectively re-identify such data." [3] • "Regular audits should be conducted to ensure ongoing compliance [with all relevant regulations]."[9] • "The patchwork of Canadian privacy laws can make it difficult to mobilize good quality, diverse datasets of personal health information from across Canada for the purposes of AI training."[4]
Section C3: Technical Security	Monitoring, maintenance, and sustainability.	Vector Institute[9] emphasizes that measures to secure data are defined (e.g., encryption methods, access controls, firewalls). "Regular audits should be conducted to ensure data security" (i.e., a component of the sustainability strategy of the AI tool).[9]

Section C4: Interoperability criteria	Technical infrastructure and integration.
	
	Monitoring, maintenance, and sustainability.
		<u>Technical infrastructure and integration.</u>
		• Define the integration points. "An integration point is where an ML solution interfaces with existing health care infrastructure. Having a proper integration point with the clinical workflow and systems is crucial for health care deployment of AI solutions, as it ensures that these systems effectively augment medical professionals' decision-making, enhancing efficiency, and improving patient outcomes without disrupting existing processes that need to be preserved. How does your solution fit into the current clinical workflow and existing IT systems? You may want to create a visual representation (e.g., flowchart, steps, process map) clearly indicating where pain points exist in your process"[9]
		• What is your technical integration strategy? [9] "When setting up a data pipeline during the development process, the needs of the production environment should be considered to account for the type of data that will be input. It is also important to consider mitigation techniques, monitor for potential errors, and account for variation in the amount of data your model processes. Think about your data sources. What data sources and types are available at the time of decision-making? What is your sample size? How did you handle missing data? Can you explain how your predictions were calculated?"[9]
		• "Scalibility: The system should be designed to scale" (i.e., handling increased data, expanding to additional use cases or departments within the organization) and the "architecture and infrastructure should be robust enough to support this growth."[9]
		• Best practice examples from the Vector Institute for setting up a data pipeline in production:
		  ○ start with a clear understanding of pipeline requirements (e.g., understanding data sources, data formats, processing, storage and output requirements),
		  ○ use scalable and flexible technologies to accommodate changing data volumes and requirements (e.g., cloud platforms, big data frameworks),
		  ○ Assess whether all the features in your model are required for adequate performance (Design for the simplest model possible with the lowest amount

		of features to reduce overfitting, improve model interpretability, and optimize for long-term maintenance of the ML model) ○ Use automated testing and validation to ensure that the data pipeline is working correctly: ○ Ensure data security and compliance in your pipeline. Data should be protected using appropriate security measures, including encryption and access controls. Data de-identification should occur early in the data pipeline, such that personally identifiable information is removed or transformed before data is used for analysis or storage. Ensure that the pipeline is compliant with relevant regulations and standards. ○ Implement monitoring and alerts to detect and address any issues with the data pipeline in a timely manner: Set up monitoring and alerts for key metrics, such as data volume, processing times, and error rates, then establish processes for responding to alerts ○ Document the data pipeline to ensure that everyone involved in its development and maintenance understands how it works: Document the data sources, processing steps, storage systems, and output formats. Keep the documentation up to date as the pipeline evolves. ○ Plan for ongoing maintenance and updates to the data pipeline[9] <u>Monitoring, maintenance, and sustainability.</u> • Health Canada's draft guidance reiterates the need for manufacturers of MLMD to provide performance/bench testing or software verification and validation information (e.g., evidence to support inter-compatibility with all supported input and output devices).[7] A few examples of interoperability considerations as part of a sustainability strategy for an AI tool: (i) the AI system should fit seamlessly into the existing clinical workflows to minimize disruption to the current system, which reduces resistance and improves the likelihood of long term adoption; and (ii) AI applications should be user-friendly following best practices for user-centred design, integrate smoothly with existing systems to encourage widespread adoption, should be easy to use and understand for end users (clinicians, medical staff, patients).[9]
Section D1: Usability and accessibility	Transparency, explainability, and intelligibility. Inclusiveness, equity, and bias. Responsibility and accountability.	<u>Transparency, explainability, and intelligibility</u>. • Ensure transparency, explainability and intelligibility. AI technologies should be explainable to the extent possible and according to the capacity of those to whom the explanation is directed.[12] "Transparency requires that sufficient information be published or documented before the design and deployment of an AI technology. Transparency requirements should consider various people involved in patient health care across the lifecycle of the device (e.g., patients, users, health care providers, and regulators)."[12] • Example best practices for transparency and explainability polices and procedures from Canada Health Infoway: "Establish a process of user engagement to assess what

	Monitoring, maintenance, and sustainability.	would constitute a meaningful explanation. Document the explanations that have been identified as useful by your users. Documenting these findings could be useful for your own accountability and auditing purposes." "Identify within your organization those that will be accountable to manage and oversee explainability requirements. Ensure that you have a designated human point of contact for individuals if they may want more information or to contest a decision or output made by the system."[4] • Example questions from Canada Health Infoway for AI vendor assessment: "Does the vendor have a knowledge plan to ensure that your organization will be able to effectively use the tool on their own?"[4] "Will the vendor use customized algorithms and provide information on their model-building methodology (e.g., how do they select variables? What testing and validation processes are used?)? How explainable are the outputs of the system? What mechanisms does the vendor propose to make the system more transparent and explainable (e.g., disclosing what training data was used, which variables contributed most for a specific outcome and data quality tests conducted to ensure that the system performs as intended). Would the vendor consider using additional technology solutions (sometimes called XAI "explainable AI tools") to increase transparency and explainability of system outputs? What additional information about the system is the vendor prepared to make available to users?"[4] • Example questions from Canada Health Infoway that organizations could ask in assessing potential risks of AI system, related to transparency and explainability: "What techniques will be used by the system (e.g., rules-based versus ML)?" What explanations will be given to internal and external knowledge users? "Is the system's technique compatible with the required level of explainability (e.g., consider that deep learning techniques may yield lower levels of explainability)? Where appropriate, can system outputs be translated into plain-language explanations? Is there a recourse mechanism for patients or other external knowledge users that wish to challenge a system output?" "Is information about the system shared with patients to help them [consent/patient-centric considerations] make informed choices prior to engaging with it?"[4] • Registered Nurses' Association of Ontario's best practice guideline on clinical practice in the digital health environment largely focused on educating, collaborating, and consulting with end users (i.e., nurses and other health care providers) to align with clinical workflows and effectively meet end users' needs. For example, education training could include understanding how AI gathers data to make decisions, emphasizing AI tools are not intended to replace health providers' critical thinking or clinical judgment, and understanding algorithmic biases present in AI tools that may perpetuate health inequalities.[2] • "What steps have you taken to ensure that the AI model is interpretable and explainable and that all users can understand its decision-making process?"[9]
		Inclusiveness, equity, and bias.

- Excerpts from World Health Organization's Ethics and Governance of AI of Health: "Inclusiveness requires that AI used in health care is designed to encourage the widest possible appropriate, equitable use and access, irrespective of age, gender, income, ability or other characteristics."[12] "AI technologies should not be biased. Bias is a threat to inclusiveness and equity because it represents a departure, often arbitrary, from equal treatment."[12] "AI developers should ensure that AI data, and especially training data, do not include sampling bias and are therefore accurate, complete and diverse." "AI technologies should minimize inevitable power disparities between providers and patients or between companies that create and deploy AI technologies and those that use or rely on them." "The effects of use of AI technologies must be monitored and evaluated, including disproportionate effects on specific groups of people when they mirror or exacerbate existing forms of bias and discrimination."[12]
- Examples of necessary risk management for bias from Health Canada's draft guidance document: "Over the lifecycle of the MLMD, manufacturers should apply sex and gender-based analysis plus and consider the unique anatomical, physiological, and identity characteristics of patients" (i.e., design; risk management; data selection and management; development and training; testing and evaluation; clinical validation; transparency; and post-market performance monitoring).[7] "This includes taking into consideration sex and gender, racial and ethnic minorities, elderly and pediatric populations, and pregnant people; and collecting and analyzing disaggregated data on sub-populations in clinical studies, training data and test data, as appropriate."[7]
- "Clinical Study Participants and Data Sets Are Representative of the Intended Patient Population: Data collection protocols should ensure that the relevant characteristics of the intended patient population (for example, in terms of age, gender, sex, race, and ethnicity), use, and measurement inputs are sufficiently represented in a sample of adequate size in the clinical study and training and test datasets so that results can be reasonably generalized to the population of interest. This is important to manage any bias, promote appropriate and generalizable performance across the intended patient population, assess usability, and identify circumstances where the model may underperform."[11]
- The Canadian Law & HTA Working Group presents considerations for HTA Bodies: "Is the technology under consideration a health-related AI application, and if so, does" the technology present a risk of bias, discrimination (e.g., gender, age or income level) or violation of privacy that requires further assessment?"[10] "Racial bias is present in non-AI medical devices, and this data may be used to develop AI devices. Further, if health-related ML applications are trained on data that is non-representative, excluding marginalized patients, this could reinforce or worsen existing discriminatory treatment within the health care system. Health Canada's apparent failure to explicitly address algorithmic bias as a safety requirement could perpetuate existing disparities for marginalized populations."[10]
- Registered Nurses' Association of Ontario's best practice guideline noted certain health equity considerations, including the high cost of AI-driven predictive analytics systems and the feasibility of implementing these systems.[2]
- Canadian Association of Radiologists also highlights the importance of legal and ethical issues related to AI (in medical imaging), related to patient data (privacy, confidentiality,

ownership, and sharing), algorithms (levels of autonomy, liability, and jurisprudence); practice (best practices and current legal framework). [6]

- The Vector Institute highlights the following: “Ensure that both the validation and test data are diverse and representative of the population that the model is intended to serve: The test data should include a broad range of patient characteristics and clinical scenarios that are representative of the intended population(s).” [For example, “Have you ensured that your AI model has been trained on diverse and representative datasets, such that it can generalize to new and unseen data?”] Consider various age groups, genders, geographic regions, comorbidities, etc. This will help to ensure that the model can generalize well to new and unseen data, improving predictive accuracy. In addition, your validation set should also capture your deployment environment.”[9]

Responsibility and accountability.

- Foster responsibility and accountability. **“**Responsibility can be assured by application of “human warranty”, which implies evaluation by patients and clinicians in the development and deployment of AI technologies. When something does go wrong in application of an AI technology, there should be accountability.”[12]
- Accountability (e.g., during AI vendor assessment, the Vector Institute states: ask the vendor if they allow third-party audits of their AI system to check for data quality and bias)[9]
- Canadian Association of Radiologists also highlights “guidelines will be required prior to the deployment of AI assistive tools in hospital departments to minimize the potential harm and liability for malpractice in case of medical error involving AI.”[6]

User buy-in and organizational readiness.

Organizational readiness also includes a change management strategy.

- “What is your change management strategy? Do you have buy-in from your clinical users, informatic users, and senior leadership?”[9] Vector Institute describes the importance of having “a concrete change management strategy when deploying and implementing AI models in a clinical setting”.
- Do you have buy-in from your clinical users (e.g., patients, clinicians, organization) in the context of deploying AI models in health care? Vector Institute discusses clinical champions, a shared vision, evidence of effectiveness, training and support, trust and transparency, communication, feedback mechanisms, and regulatory compliance, ethics, and privacy.[9]
- Do you have buy-in from your informatics users (e.g., a multi-disciplinary team of in the areas of data science and analytics, IT infrastructure, data management, application development, information security, clinical informatics, and quality assurance)?
- Do you have buy-in from senior leadership from multiple departments?[9]
- Vector Institute highlights these points when communicating with senior leadership team: strategic alignment, demonstrated value, risk assessment, budget allocation,

change management, communication, regulatory compliance, long-term vision, user engagement, return on investment.[9]

- Example risk assessment questions from Canada Health Infoway regarding organizational readiness: "will the AI system affect current employee roles and responsibilities, will it lead to workforce redundancies? Will employees need new training? Are existing policies adequate to cover the safe and effective operationalization of the system? Does the organization have the right talent mix to manage the system internally?" Consider reputational impact, including: "If the system does not operate as intended, could it lead to negative media coverage or impact the trustworthiness of the organization? If the system does not operate as intended, could it negatively impact patients' expected standard of care?"[4]
- Canada Health Infoway suggests implementors of an AI present change management considerations, including to "anticipate how AI systems can impact the morale of your organization, identify employee training needs, develop change management strategies to support a more robust innovation strategy."[4] Examples of policies and procedures include policies on change management and training manuals.[4]

<u>Monitoring, maintenance, and sustainability.</u>

- Example of a question from Canada Health Infoway for AI vendor assessment: "What human oversight mechanisms does the vendor have in place (e.g., are there measures in place that would enable a human to effectively intervene in, override or reverse system outputs?"[4]
- Example questions from Canada Health Infoway for bias and non-discrimination assessment during deployment and monitoring: "Define triggers that will automatically alert those responsible for oversight and monitoring of the AI system should the AI system begin to behave unexpectedly; if automatic triggers are not possible, define how often the AI system should undergo re-validation to ensure it remains free from bias and robust; document acceptable use criteria for the AI system to ensure the system is only deployed in an appropriate context; consider algorithmic auditing by third parties to ensure that your AI system remains free from bias; if indicators of unwanted bias are found in the system, immediately retrain, or re-develop the system."[4]
- "Deployed Models Are Monitored for Performance and Re-training Risks are Managed: Deployed models have the capability to be monitored in "real world" use with a focus on maintained or improved safety and performance. Additionally, when models are periodically or continually trained after deployment, there are appropriate controls in place to manage risks of overfitting, unintended bias, or degradation of the model (for example, dataset drift) that may impact the safety and performance of the model as it is used by the Human-AI team."[11]
- Example components from the Vector Institute of the sustainability strategy of the AI tool related to usability and accessibility: AI applications should be user-friendly following best practices for user-centred design, integrate smoothly with existing systems to encourage widespread adoption, should be easy to use and understand for

	end users (clinicians, medical staff, patients). Provide regular training and support for users to promote adoption.[9]

AI = aritificial intelligence; CDA-AMC = Canada's Drug Agency – L'Agence des médicaments du Canada; DTAC = Digital Technology Assessment Criteria.

Patient Engagement

Table 4: Summary of Patient Engagement Using the Guidance for Reporting Involvement of Patients and the Public (version 2) Short Form Reporting Checklist[62]

Section and topic	Item	Report section
Aim	One patient contributor participated in a one-hour interview during the drafting phase of the report to highlight her experiences, perspectives, and priorities for the use of AI in stroke detection.	Methods
Methods	After giving informed consent, 1 patient contributor discussed her experience of a stroke and her perspectives on the use of AI in stroke detection.	Methods
Results of engagement	**Perspectives Shared** The patient contributor shared her personal experience of having a hemorrhagic stroke, the emergency treatment she received, and her recovery. She did not know whether AI had been used in her diagnosis. **RapidAI** RapidAI was described to the patient contributor, and she shared her thoughts on its use in stroke detection, relating to perceived potential outcomes and ethical considerations as described below. **Outcomes to Measure** *Speed* Two of the potential benefits that the patient contributor hoped for was speed and accuracy. She was hopeful that if the use of AI meant a speedier and more accurate diagnosis, perhaps clinicians could initiate the most appropriate treatment sooner. She hoped that this would reduce the damage being caused by the stroke and improve outcomes. *Accuracy* When asked to expand on her comment about accuracy being crucial to the success of using AI, the patient contributor posited that, while ensuring the accuracy of the AI technology was a concern, she was curious about whether AI could accurately identify issues earlier than a clinician, or perhaps prevent human error. *Other Outcomes* When asked specifically about outcomes of interest, speed and accuracy were the patient contributor's priorities. However, she also identified minimizing the damage caused by strokes and mortality rates as other factors to consider. **Ethical Considerations** *Equitable Access* The patient contributor expressed concern about the accessibility of RapidAI technologies outside of major stroke centres and wondered whether all major hospitals could benefit from this technology to assist in triaging (and potentially transferring) patients more quickly. She also had concerns about services in rural and remote community hospitals. *Privacy*	Summary of Findings

Section and topic	Item	Report section
	The patient contributor suggested that, in a crisis, she felt that most people wouldn't be thinking of ethical considerations like privacy and data sharing – they would be focused on diagnosis, treatment, and survival. The patient contributor reflected that some people may be more reluctant to have her personal information shared with the manufacturer, while others may be used to sharing her personal information with cell phone or computer software manufacturers. She suggested that there may be a divide, with some individuals being more protective of her personal information and others more familiar with novel technologies and sharing her data. Regardless of the level of patient comfort with sharing data, the patient contributor shared concerns about privacy, safety of information, accuracy, and reliability of storage. *Informing the Patient* The patient contributor expressed curiosity about whether patients will be informed that her clinicians used AI in her diagnosis. She herself did not know whether the technology was in use at the time of her stroke.	
Discussion and conclusions	Success of engagement in this review is related to several factors. Firstly, there was outreach through several organizations. Secondly, the patient contributor was briefed on the objectives of the project in an introductory call and supported by a Patient Engagement Officer. Thirdly, 3 of the project team members attended the interview to hear from the individual directly and to engage her in conversation. Fourthly, a gift card was offered as a gesture of appreciation for her contribution. Finally, the patient contributor was offered the opportunity to be thanked by name in the acknowledgements section of the report or to remain anonymous. She preferred to remain anonymous. However, there were limitations. Though we had intended to engage with 3 individuals, 2 patients and a clinician, we had limited response to our outreach, and the sole clinician who responded to our initial request ultimately declined to participate due to time constraints.	Limitations
Critical Reflections	The patient contributor was highly engaged in the discussion, sharing her experience, thoughts, and priorities. Questions were sent ahead of time so that she could prepare. A summary of the discussion was drafted and sent to the patient contributor. She was able to share feedback and approve the summary as an accurate reflection of the conversation. One limitation of our approach is that people need access to reliable technology, phone, and internet access to contribute to our work, which may exclude some voices.	Limitations

AI = artificial intelligence.

References of Potential Interest

Preliminary Frameworks and/or Guidance

Implementation frameworks for end-to-end clinical AI: derivation of the SALIENT framework. Journal of the American Medical Informatics Association, Volume 30, Issue 9, September 2023, Pages 1503–1515. https://academic.oup.com/jamia/article/30/9/1503/7174318

Truong T, Gilbank P, Johnson-Cover K, Ieraci A. A Framework for Applied AI in Healthcare. InMedInfo 2019 Aug 1 (pp. 1993-1994).

Knowledge User Perspectives

Zhou K, Gattinger G. The Evolving Regulatory Paradigm of AI in MedTech: A Review of Perspectives and Where We Are Today. Ther Innov Regul Sci. 2024 May;58(3):456-464. PubMed: PM38528278. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11043174

Silcox C, Zimlichmann E, Huber K, et al. The potential for artificial intelligence to transform healthcare: perspectives from international health leaders. NPJ Digit Med. 2024 Apr 9;7(1):88. PubMed: PM38594477. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11004157

Alami H, Rivard L, Lehoux P, Ag Ahmed MA, Fortin JP, Fleet R. Integrating environmental considerations in digital health technology assessment and procurement: Stakeholders' perspectives. Digital Health. 2023 Dec;9:20552076231219113. https://journals.sagepub.com/doi/pdf/10.1177/20552076231219113

Hogg HDJ, Al-Zubaidy M, Talks J, et al. Stakeholder Perspectives of Clinical Artificial Intelligence Implementation: Systematic Review of Qualitative Evidence. J Med Internet Res. 2023 Jan 10;25:e39742. PubMed: PM36626192. https://www.jmir.org/2023/1/e39742/

Whittaker R, Dobson R, Jin CK, et al. An example of governance for AI in health services from Aotearoa New Zealand. NPJ Digit Med. 2023 Sep 1;6(1):164. PubMed: PM37658119

References

1. Therapeutic Goods Administration. Artificial Intelligence (AI) and medical device software: Information for software manufacturers about how we regulate AI medical devices. Canberra (AUS): Commonwealth of Australia; 2024: https://www.tga.gov.au/how-we-regulate/manufacturing/manufacture-medical-device/manufacture-specific-types-medical-devices/software-based-medical-devices/artificial-intelligence-ai-and-medical-device-software Accessed 2024-06-18.
2. Best Practice Guideline: Clinical Practice in a Digital Health Environment. Toronto (ON): Registered Nurses' Association of Ontario; 2024: https://rnao.ca/bpg/guidelines/clinical-practice-digital-health-environment. Accessed 2024 Jun 17.
3. Digital Health Solutions Privacy & Security Guideline. Toronto (ON): Canada Health Infoway; 2023: https://www.infoway-inforoute.ca/en/component/edocman/resources/reports/privacy/6475-digital-health-solutions-privacy-security-guideline?Itemid=103#:~:text=This%20Guideline%20sets%20out%20technical,and%20secure%20information%20handling%20processes. Accessed 2024 Jun 17.
4. Toolkit for Implementers of Artificial Intelligence in Health Care. 2nd ed. Toronto (ON): Canada Health Infoway; 2023: https://www.infoway-inforoute.ca/en/component/edocman/resources/artificial-intelligence/3998-toolkit-for-implementers-of-artificial-intelligence-in-health-care?Itemid=101. Accessed 2024 Jun 17.
5. Artificial Intelligence. Ottawa (ON): Canadian Association of Radiologists: https://car.ca/innovation/artificial-intelligence/. Accessed 2024 Jul 5.
6. Canadian Association of Radiologists Artificial Intelligence Working Group. Canadian Association of Radiologists white paper on ethical and legal issues related to artificial intelligence in radiology. *Canadian Association of Radiologists' Journal.* 2019;70(2):107-118.
7. Health Canada. Draft guidance document: Pre-market guidance for machine learning-enabled medical devices. Ottawa (ON): Government of Canada; 2023: https://www.canada.ca/content/dam/hc-sc/documents/services/drugs-health-products/medical-devices/application-information/guidance-documents/pre-market-guidance-machine-learning-enabled-medical-devices/pre-market-guidance-machine-learning-enabled-medical-devices.pdf. Accessed 2024 Jun 18.
8. Medicines and Healthcare Products Regulatory Agency. Guidance: Software and AI as a Medical Device Change Programme. London (GB): Gov.UK; 2023: https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme. Accessed 2024 Jun 18.
9. Dhalla A, Akinli Kocak S, Wan F, Da Silva J, Jain T. Vector Institute Health AI Implementation Toolkit. Toronto (ON): Vector Institute; 2023: https://vectorinstitute.ai/health-ai-implementation-toolkit/. Accessed 2024 Jun 14.
10. Legal Guidance for HTA Bodies. Canadian Law & HTA Working Group; 2022: https://drive.google.com/file/d/1nxsf4HRP9xYZaDi6oXmwB5YyberIbpHv/view. Accessed 2024 Jun 21.
11. Health Canada. Good Machine Learning Practice for Medical Device Development: Guiding Principles. Ottawa (ON): Government of Canada; 2021: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/good-machine-learning-practice-medical-device-development.html. Accessed 2024 Jun 19.
12. Ethics and governance of artificial intelligence for health. Geneva (CHE): World Health Organization; 2021.
13. Generating evidence for artificial intelligence-based medical devices: a framework for training, validation and evaluation. Geneva (CHE): World Health Organization; 2021: https://iris.who.int/bitstream/handle/10665/349093/9789240038462-eng.pdf?sequence=1. Accessed 2024 Jun 18.
14. LPPR: Dossier submission to the Medical Device and Health Technology Evaluation Committee (CNEDiMTS). Saint-Denis (FR): Haute Autorité de Santé; 2020: https://www.has-sante.fr/upload/docs/application/pdf/2020-10/guide_dm_vf_english_publi.pdf. Accessed 2024 Jun 18.
15. Health Canada. Guidance Document: Pre-market Requirements for Medical Device Cybersecurity. Ottawa (ON): Government of Canada; 2019: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/cybersecurity/document.html. Accessed 2024 Jun 27.
16. Health Canada. List of recognized standards for medical devices. Ottawa (ON): Government of Canada; 2022: https://www.canada.ca/content/dam/hc-sc/documents/services/drugs-health-products/medical-devices/standards/list-recognized-standards-medical-devices-guidance/list-recognized-standards-medical-devices-guidance.pdf. Accessed 2024 Jul 2.
17. Department of Justice Canada. 2021, Medical Devices Regulations: SOR/98-282. Ottawa (ON): Government of Canada; 2021: https://laws-lois.justice.gc.ca/eng/regulations/sor-98-282/. Accessed 2024 Jun 16.
18. Health Canada. Safe medical devices in Canada. Ottawa (ON): Government of Canada; 2022: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/fact-sheets/safe-medical-devices-fact-sheet.html. Accessed 2023 Jun 27.
19. Health Canada. Mandatory Medical Device Problem Reporting Form for Industry. Ottawa (ON): Government of Canada; 2018: https://www.canada.ca/en/health-canada/services/drugs-health-products/medeffect-canada/adverse-reaction-reporting/mandatory-medical-device-problem-reporting-form-industry-adverse-reaction-reporting.html. Accessed 2024 Jul 2.

20. Health Canada. Incident reporting for medical devices: Guidance document. Ottawa (ON): Government of Canada; 2021: https://www.canada.ca/en/health-canada/services/drugs-health-products/reports-publications/medeffect-canada/incident-reporting-medical-devices-guidance-2021.html. Accessed 2024 Jul 1.
21. Report a medical device problem (for health care professionals). Ottawa (ON): Government of Canada; 2021: https://hpr-rps.hres.ca/side-effects-reporting-form.php?form=medical_devices#:~:text=Reporting%20by%20hospitals%20is%20required,being%20documented%20within%20the%20hospital. Accessed 2024 Jul 2.
22. Health Canada. Medical device application and report forms. Ottawa (ON): Government of Canada; 2024: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/forms.html. Accessed 2024 Jul 2.
23. Health Canada. Declaration of Conformity. Ottawa (ON): Government of Canada; 2006: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/forms/declaration-conformity-forms-medical-devices.html. Accessed 2024 Jul 2.
24. Health Canada. Guidance Document: Software as a Medical Device (SaMD): Definition and Classification Vol Government of Canada: Ottawa (ON); 2019: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/software-medical-device-guidance-document.html. Accessed 2024 Jun 16.
25. Health Canada. Compliance and enforcement of medical devices - Forms, guidance, policies and laws. Ottawa (ON): Government of Canada; 2023: https://www.canada.ca/en/health-canada/services/drugs-health-products/compliance-enforcement/information-health-product/medical-devices.html. Accessed 2024 Jul 2.
26. PIPEDA requirements in brief. Ottawa (ON): Office of the Privacy Commissioner of Canada; 2024: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/. Accessed 2024 Jun 17.
27. Provincial laws that may apply instead of PIPEDA. Ottawa (ON): Office of the Privacy Commissioner of Canada; 2020: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/. Accessed 2024 Jun 17.
28. PIPEDA Self-Assessment Tool. Ottawa (ON): Office of the Privacy Commissioner of Canada; 2021: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/pipeda_sa_tool_200807/. Accessed 2024 Jun 17.
29. A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations. Victoria (BC): Office of the Information & Privacy Commissioner for British Columbia; 2015: https://www.oipc.bc.ca/documents/guidance-documents/1371. Accessed 2024 Jun 17.
30. PIPA: 10 Steps to Implement PIPA. Edmonton (AB): Office of the Information and Privacy Commissioner of Alberta; 2010: https://oipc.ab.ca/resource/pipa-implementation/. Accessed 2024 Jun 17.
31. National Assembly of Québec. Bill 64, chapter 25: An Act to modernize legislative provisions as regards the protection of personal information. *First Session. Forty-Second Legislature*. Québec (QC): Québec Official Publisher; 2021: https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/en/2021/2021C25A.PDF. Accessed 2024 Jun 17.
32. Privacy impact assessments for the private sector. Victoria (BC): Office of the Information & Privacy Commissioner for British Columbia; 2020: https://www.oipc.bc.ca/documents/guidance-documents/2246. Accessed 2024 Jul 3.
33. Privacy impact assessment (PIA) template for organizations. Victoria (BC): Office of the Information & Privacy Commissioner for British Columbia; 2020: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.oipc.bc.ca%2Fdocuments%2Fguidance-documents%2F2245&wdOrigin=BROWSELINKhttps://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.oipc.bc.ca%2Fdocuments%2Fguidance-documents%2F2245&wdOrigin=BROWSELINK. Accessed 2024 Jul 3.
34. Digital Privacy Impact Assessment (DIPA). Victoria (BC): Government of British Columbia; 2024: https://pia.gov.bc.ca/. Accessed 2024 Jun 28.
35. Privacy Impact Assessments. Edmonton (AB): Office of the Information and Privacy Commissioner of Alberta: https://oipc.ab.ca/privacy-impact-assessments/. Accessed 2024 Jul 3.
36. General Privacy Law | Private Sector - Government of Alberta | Alberta's Personal Information Protection Act (PIPA) https://open.alberta.ca/publications/p06p5. Accessed 2024-06-28.
37. Guidelines for processing personal data across borders. Ottawa (ON): Office of the Privacy Commissioner of Canada; 2009: https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/. Accessed 2024 Jun 17.
38. Innovation, Science and Economic Development Canada. CyberSecure Canada. Ottawa (ON): Government of Canada; 2024: https://ised-isde.canada.ca/site/cybersecure-canada/en. Accessed 2024 Jun 28.
39. Baseline Cyber Security Controls for Small and Medium Organizations. Ottawa (ON): Digital Governance Council; 2021: https://dgc-cgn.org/standards/find-a-standard/standards-in-cybersecurity/cybersecurity-smes/. Accessed 2024 Jul 2.

40. Get Cyber Safe Guide for Small and Medium Businesses. Ottawa (ON): Government of Canada; 2022: https://www.getcybersafe.gc.ca/en/resources/get-cyber-safe-guide-small-and-medium-businesses. Accessed 2024 Jun 28.
41. Canadian Centre for Cyber Security. Security considerations for your website (ITSM.60.005). Ottawa (ON): Government of Canada; 2021: https://www.cyber.gc.ca/en/guidance/security-considerations-your-website-itsm60005#wb-tphp. Accessed 2024 Jul 2.
42. Canadian Centre for Cyber Security. Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035). Ottawa (ON): Government of Canada; 2024: https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035. Accessed 2024 Jul 2.
43. Open Worldwide Application Security Project. OWASP Top Ten. 2021; https://owasp.org/www-project-top-ten/.
44. Penetration Testing Methodologies. *The OWASP Testing Framework*: Open Worldwide Application Security Project: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies. Accessed 2024 Jul 2.
45. Secure development and deployment guidance. London (GB): National Cyber Security Centre: https://www.ncsc.gov.uk/collection/developers-collection/principles/produce-clean-maintainable-code. Accessed 2024 Jul 2.
46. Canadian Centre for Cyber Security. Network security logging and monitoring - ITSAP.80.085. Ottawa (ON): Government of Canada; 2022: https://www.cyber.gc.ca/en/guidance/network-security-logging-monitoring-itsap80085. Accessed 2024 Jul 2.
47. API Guidance. Ottawa (ON): Government of Canada; 2021 https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/enabling-interoperability/api-guidance.html. Accessed 2024 Jul 3.
48. Treasury Board of Canada Secretariat. Government of Canada Standards on APIs. Ottawa (ON): Government of Canada; 2020: https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/government-canada-standards-apis.html. Accessed 2024 Jul 3.
49. Ontario Health. Digital Health Information Exchange Standard. Toronto (ON): Government of Ontario; 2022: https://www.ontariohealth.ca/system-planning/digital-standards/digital-health-information-exchange. Accessed 2024 Jul 3.
50. Enabling connection and communication across the health system. Toronto (ON): Canada Health Infoway; 2024: https://www.infoway-inforoute.ca/en/digital-health-initiatives/interoperability. Accessed 2024 Jul 3.
51. Competition Bureau Canada. Unlocking the power of health data. Ottawa (ON): Government of Canada; 2022: https://competition-bureau.canada.ca/unlocking-power-health-data. Accessed 2024 Jul 3.
52. API Security Best Practices Primer. Ottawa (ON): Government of Canada; 2021: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/enabling-interoperability/api-guidance/security.html. Accessed 2024 Jul 3.
53. OAuth 2.0. https://oauth.net/2/.
54. IEEE Standard - Health informatics -- Device interoperability -- Part 10206: Personal health device communication -- Abstract Content Information Model. Piscataway (NJ): IEEE Standards Association; 2022: https://standards.ieee.org/ieee/11073-10206/10311/#:~:text=Within%20the%20context%20of%20the%20ISO%2FIEEE%2011073%20personal%20health,between%20device%20types%20and%20vendors. Accessed 2024 Jul 3.
55. Government of Canada Digital Standards: Playbook. 2021: https://www.canada.ca/en/government/system/digital-government/government-canada-digital-standards.html. Accessed 2024-07-03.
56. Treasury Board of Canada Secretariat. Standard on Web Accessibility. Ottawa (ON): Government of Canada; 2011: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=23601. Accessed 2024 Jul 3.
57. NHS service standard. London (GB): NHS England; 2022: https://service-manual.nhs.uk/standards-and-technology/service-standard. Accessed 2024 Jul 22.
58. Regulatory considerations on artificial intelligence for health. Geneva (CHE): World Health Organization; 2023: https://iris.who.int/bitstream/handle/10665/373421/9789240078871-eng.pdf?sequence=1. Accessed 2024 Jun 18.
59. The First Nations Principles of OCAP®. Akwesasne (ON): First Nations Information Governance Centre: https://fnigc.ca/ocap-training/. Accessed 2024 Jun 15.
60. Framework for Research Engagement with First Nation, Metis, and Inuit Peoples. Winnipeg (MB): University of Manitoba; 2021: https://umanitoba.ca/health-sciences/sites/health-sciences/files/2021-01/framework-research-report-fnmip.pdf. Accessed 2024 Jun 15.
61. Inuit Qaujimajatuqangit: The Role of Indigenous Knowledge in Supporting Wellness in Inuit Communities in Nunavut Prince George (BC): National Collaborating Centre for Aboriginal Health; 2010: https://www.ccnsa-nccah.ca/docs/health/FS-InuitQaujimajatuqangitWellnessNunavut-Tagalik-EN.pdf. Accessed 2024 Jun 15.
62. Staniszewska S, Brett J, Simera I, et al. GRIPP2 reporting checklists: tools to improve reporting of patient and public involvement in research. *Bmj.* 2017;358:j3453.

ISSN: TBD

About CADTH: CADTH is an independent, not-for-profit organization responsible for providing Canada's health care decision-makers with objective evidence to help make informed decisions about the optimal use of drugs, medical devices, diagnostics, and procedures in our health care system.

Funding: CADTH receives funding from Canada's federal, provincial, and territorial governments, with the exception of Quebec.

Questions or requests for information about this report can be directed to **Requests@CADTH.ca**