Canada Health Infoway

Cybersecurity Practitioners' Guide to AI and Healthcare

First Nations Health Managers Association
November 7, 2024

Perry Kjargaard
Senior Director
Canada Health Infoway

Robert Martin
Senior Director
Canada Health Infoway

About Canada Health Infoway:

Who We Are

Independent, not-for-profit corporation, established 2001

Partner to Health Canada, playing key role in evolving Canada's health care system

Equally accountable to 14 federal, provincial, and territorial governments.

Vision, Mission & Goal

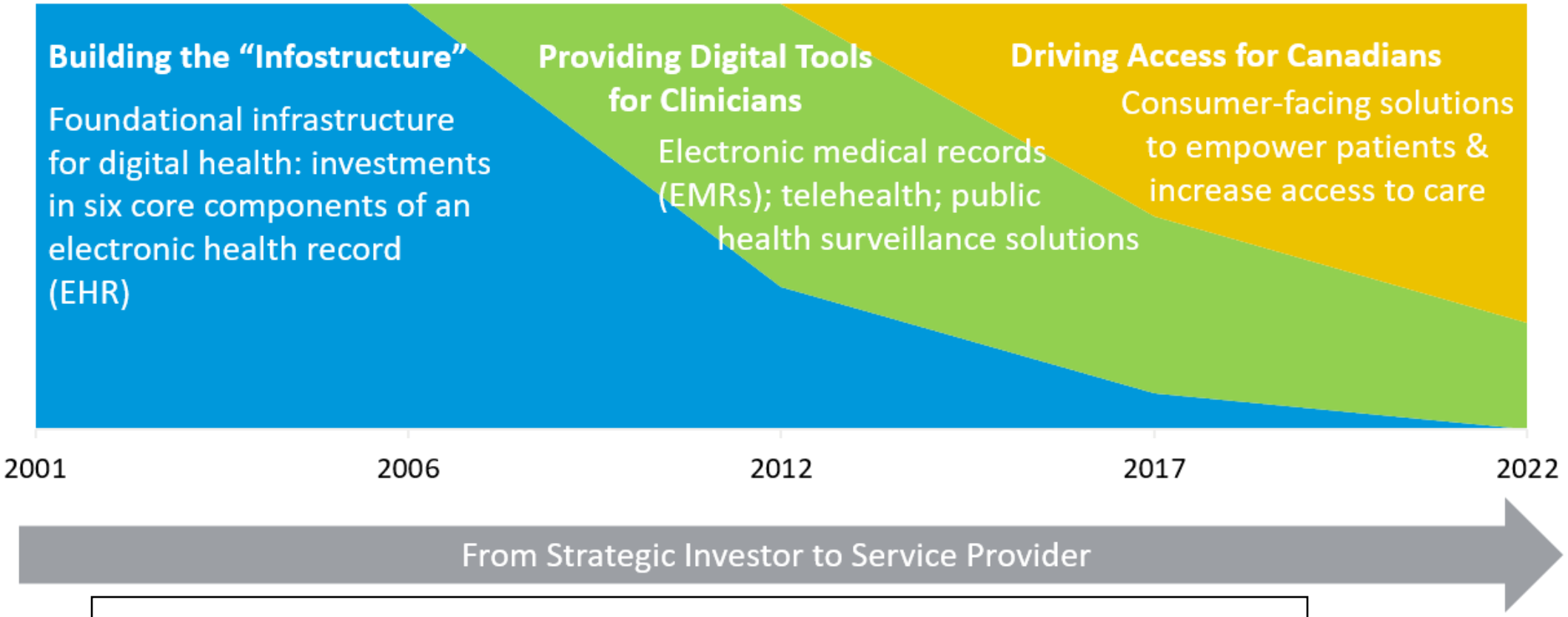
At Canada Health Infoway, we want to ensure that all Canadians have equitable access to excellent health care and health information. We believe that a more connected and collaborative system is a healthier system.

Vision:
Healthier Canadians through innovative digital health solutions.

Mission:
We mobilize Canada's health care stakeholders towards a shared and reimagined future where digital health helps create a more accessible and connected system with the patient at its heart.

Our goal is to improve health care delivery in Indigenous communities across Canada through the scale and spread of innovative digital health solutions.

The evolution of Infoway's role



Includes:

72 Initiatives directly benefiting First Nations and/or Inuit Peoples in 12 p/t's

25 Direct partnerships between Infoway and Indigenous organizations

Canada Health Infoway's Journey

©2023 Canada Health Infoway
©2022 Canada Health Infoway

Infoway Today

Infoway's Central Role

A transformation partner modernizing Canada's health care system by unlocking the value of data, mobilizing stakeholders, and fostering private and public sector collaboration.

Empowering Canadians to own their health journeys while building a patient-centric health care system.

Four Complimentary Roles

Digital Health Convenor:
Leading in digital health, AI, and standards, creating an Interoperability Centre of Excellence.

Strategic Investor:
Identifying key stakeholders and scaling digital health solutions.

Ecosystem Orchestrator:
Driving national data connectivity, standards, and innovation.

Digital Health Program Scaler: Scaling e-prescribing and advancing interoperability.

Commitment to Improving Health

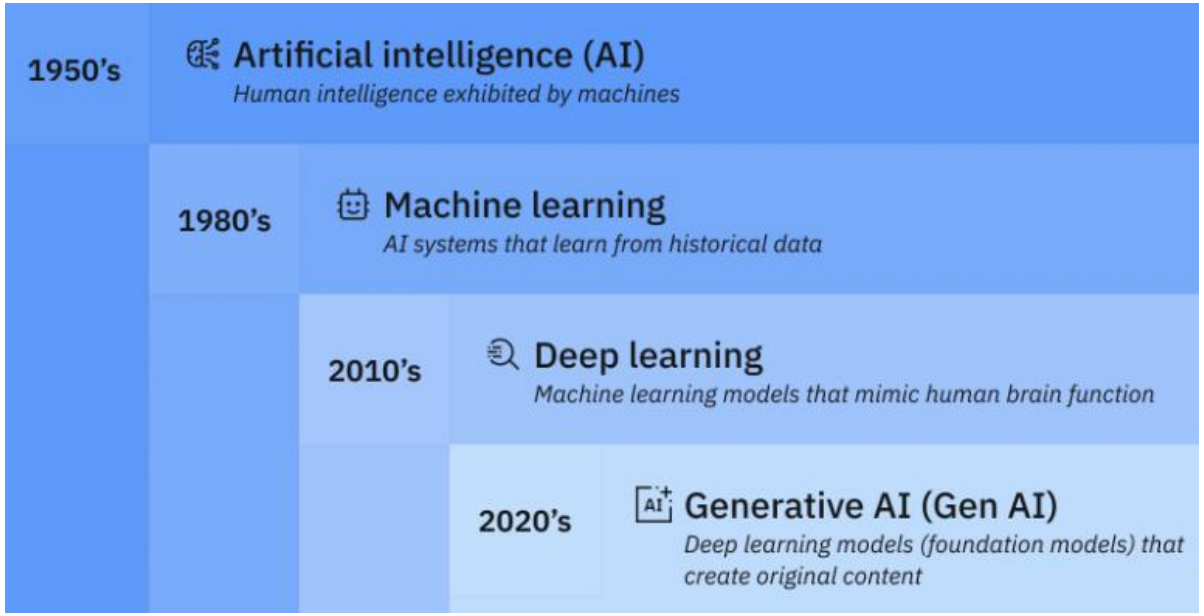
Accelerating digital health solutions adoption.

Advancing a connected care-focused health system.

Background: What is AI?

Artificial intelligence (AI) is technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity, and autonomy.

- Machine Learning (ML) involves creating models by training an algorithm to make predictions or decisions based on data.
- Deep Learning is a subset of ML that uses multilayered neural networks, that closely simulate the complex decision-making power of the human brain.
- Generative AI (Gen-AI) is learning models that can create complex original content—such as long-form text, high-quality images, realistic video or audio and more—in response to a user's prompt or request.



Source: IBM

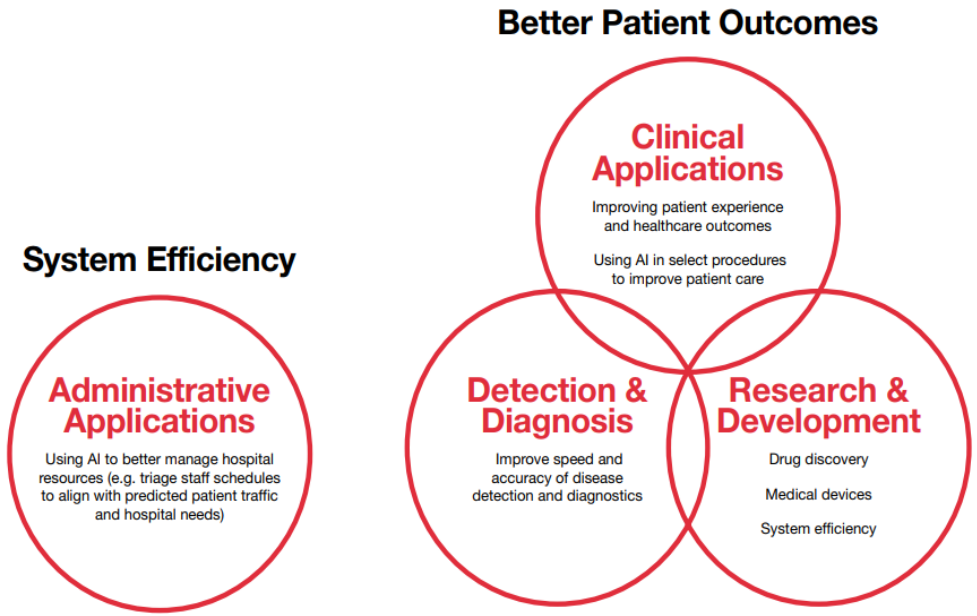
©2024 Canada Health Infoway

Canada Health Infoway

Background: the Role of AI in Healthcare

- AI adoption in healthcare is on the rise. AI can contribute to achieving the **Quadruple Aim** of healthcare:
  1. Provide better care for individuals
  2. Better health for populations
  3. At a lower per-capita cost, and
  4. Improve the work life of health care providers, including clinicians and staff.

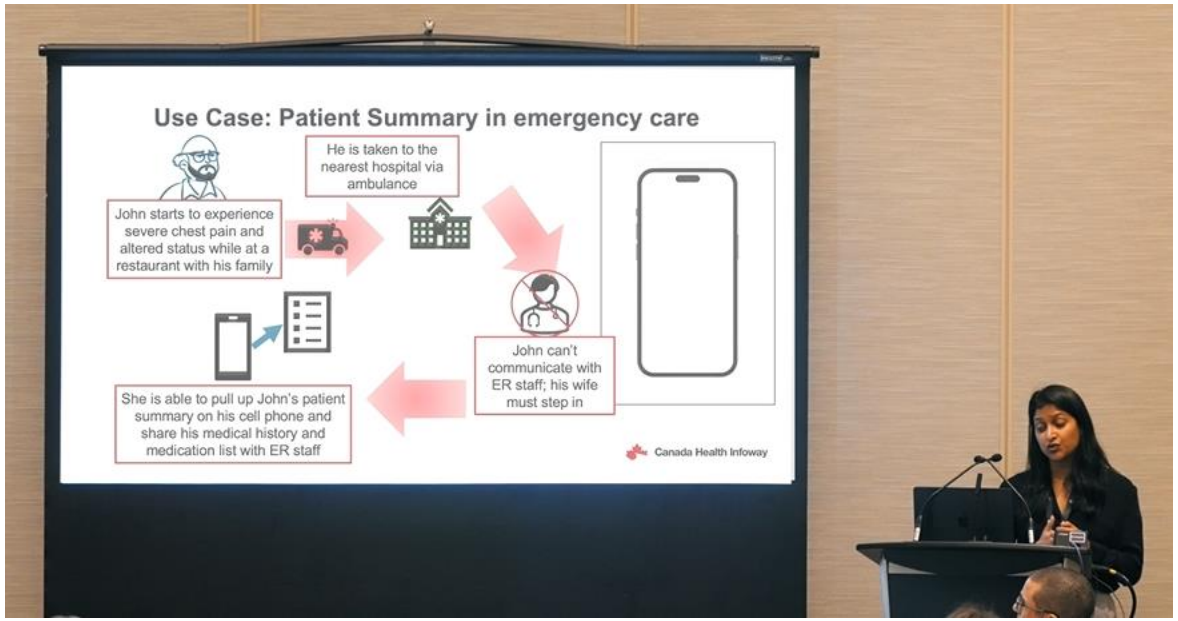
  The development and operationalization of AI is freeing healthcare professionals from repetitive tasks, augmenting clinical decision-making, and allowing more time for patient care while also improving hospital administration and the efficiency of health systems.



©2024 Canada Health Infoway

Canada Health Infoway

Patient Summary + AI Scribe use case



Infoway hosted a session called “Demonstrating the Value of the Patient Summary to Inform Care Delivery and Enable a Better Patient Experience”. In this session, the **power of AI was combined with the Patient Summary**.

Watch a short demo here.

Canada Health Infoway

Feedback from Cybersecurity Forum

- Looking for guidance around AI issues in healthcare
- Practical advice and tools for cybersecurity professionals dealing with AI
- A published working guide that will be available from Infoway

Infoway Security and AI Resources

- Infoway has already published several documents for assisting cybersecurity practitioners:
  - ***The Canada Health Infoway Privacy & Security Guideline***
    - Lists many of the security controls that can be adopted for use in a healthcare organization
    - Includes sample policies
  - ***The Canada Health Infoway AI Toolkit for Implementers***
    - Provides an overview of the issues related to the implementation and uses of AI solutions in healthcare
    - Strategic and operational guidance for designing responsible AI projects and AI governance programs

©2024 Canada Health Infoway

Canada Health Infoway

Infoway's AI Toolkit

- AI technology continues to develop rapidly
  - Not contemplated in the Toolkit:
    - Multi-modal models
    - Large Language Models (LLMs)
    - Generative AI
  - Fallback plan
    - What happens when the AI application fails
  - Weaving AI into existing applications
  - Many Hands Problem: who is responsible when AI fails?

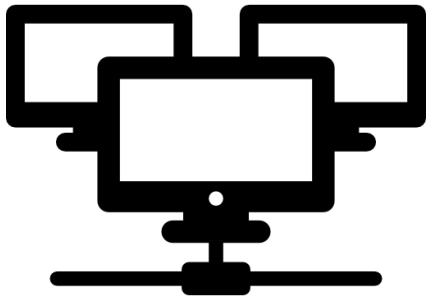
"'Adversarial machine learning' (AML), is used to describe the exploitation of fundamental vulnerabilities in ML components, including hardware, software, workflows and supply chains affecting the model's classification or regression performance > allowing users to perform unauthorised actions > extracting sensitive model information There are many ways to achieve these effects, such as prompt injection attacks in the large language model (LLM) domain, or deliberately corrupting the training data or user feedback (known as 'data poisoning')" National Cyber Security Centre (NCSC)

©2024 Canada Health Infoway

Canada Health Infoway

Project Vision - Providing Practical Guidance

- Vision for this project was to build on the Canada Health Infoway AI Toolkit with a cybersecurity lens
- Offer practical guidance for cybersecurity professionals
- Focus on the intersection of cybersecurity, AI, and healthcare from a Canadian perspective
  - Few if any resources are available with this unique lens



©2024 Canada Health Infoway

Canada Health Infoway

Guiding Questions

How do we build an infrastructure of trust to facilitate AI adoption in healthcare in a safe and responsible way?

What practical steps can cybersecurity professionals take to contribute to this infrastructure of trust?

©2024 Canada Health Infoway

Canada Health Infoway

Canada Health Infoway

Themes and Concerns

Key Themes

- AI is seen as a solution to a range of healthcare problems:
  - AI scribes and summaries – help with physician burnout
  - Better diagnostics and improved patient outcomes (e.g. AI in imaging, predictive tools)
  - More efficient and cost-effective administrative processes

- There are differences of opinion as to the degree AI will address the problems, but regardless, there will be more AI–enabled tools

©2024 Canada Health Infoway

Key Themes

- AI is quickly being woven into existing Enterprise tools (e.g. Microsoft Copilot) and EMRs
- This is in addition to 'standalone' AI tools which may have been bought or built
- Concerns over Shadow AI, similar to Shadow IT concerns we have experienced for years

©2024 Canada Health Infoway

Canada Health Infoway

Key Themes

- Concerns over increased threat risks and attacks
  - AI can be a tool for bad actors
  - Increased ransomware attacks
- All the usual issues do not go away – we still need the basics. The basics will also help address AI issues.
  - Data governance, data quality
  - Consent management
  - Interoperability
  - Digital IDs
- Costs – who will pay for the new technology (e.g. AI scribes in primary care)?

©2024 Canada Health Infoway

Canada Health Infoway

New Concerns - External

"*Attacks that either aim at **extracting data from the models** or **manipulating their decisions** are threats that need to be considered during a risk assessment. Using **pre-trained models** or publicly available datasets from external sources lowers the resources needed for developing AI systems, but may also **enable a variety of attacks**.*"

(Source – Federal Office for Information Security, Bonn)

- Large language models (generative AI) are pre-trained models which introduce new threats and types of attacks
  - Prompt injections – malicious instructions in disguise
  - Jailbreaks – prompting the model to over-ride safety guardrails

©2024 Canada Health Infoway

Canada Health Infoway

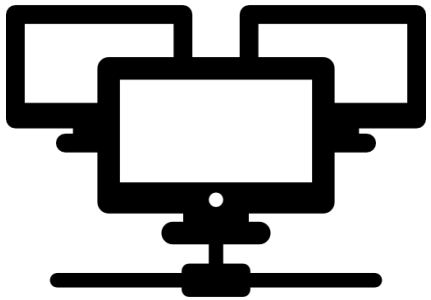
New Concerns - Internal

- Explainability – we do not always know how models work
  - Especially true of Generative AI
- User errors
  - Oversharing data (data leakage)
  - More users = more risk
- Automation Bias – propensity for people to over-rely on or over-trust machine outputs
- Data issues – for example, summarization may introduce errors or biases – might not always be obvious. This may compound over time

©2024 Canada Health Infoway

Monitoring AI

- Cybersecurity professionals will need to use tools to monitor AI
  - AI will lead to the creation of more access log data
  - Use new tools to monitor the vast amounts of new access log data to ensure usage behaviour adheres to norms
  - Determine a reasonable level of risk aligned with organizational risk appetite
  - Cybersecurity professionals need to understand the budget implications of a new AI monitoring tool



©2024 Canada Health Infoway

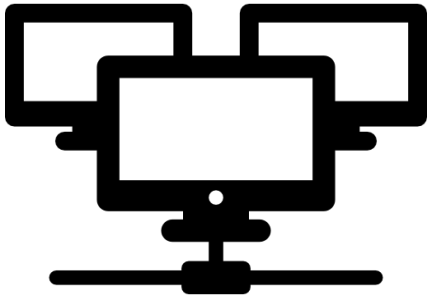
Canada Health Infoway

Canada Health Infoway

Use Case

AI Ambient Scribe Technology

- What is Ambient Scribe?
  - Creates clinical documentation of a patient's visit – either the conversation or the clinician's summary through an AI-enabled recording
  - Will extract the medically relevant information from the conversation and generate a note for inclusion in the patient's record



- Noted as a potential time-saving device that will reduce the administrative burden on healthcare practitioners

©2024 Canada Health Infoway

Canada Health Infoway

AI Ambient Scribe Technology

- Have you encountered this software in your day-to-day activities or received requests for its use by staff?

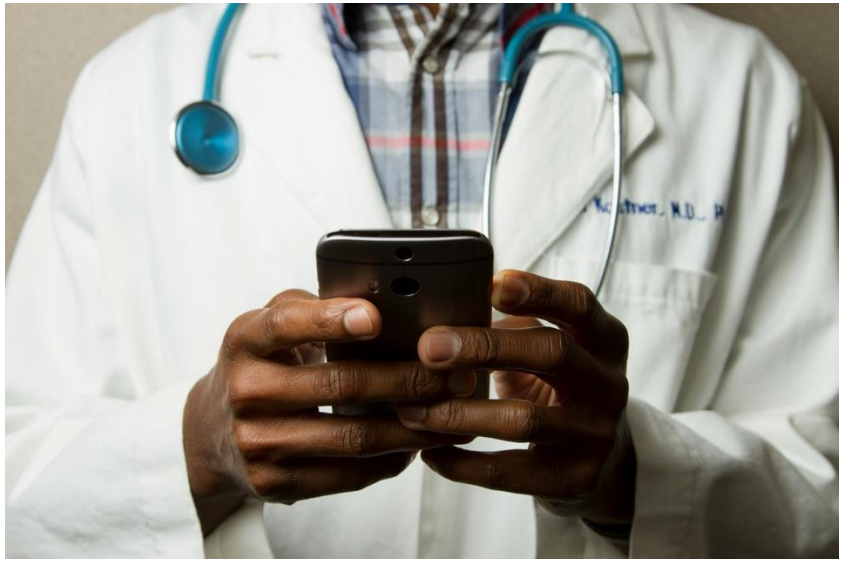
- What concerns do you feel the scribe technology raises?

©2024 Canada Health Infoway

Canada Health Infoway

Ambient Scribe Cybersecurity Risks

- Continuous collection and analysis of patient data raises the risk of data leaks and hacking
- Technology may not accurately record the contents of the visit
- Biases can be unexpectedly introduced by the AI software
- Data could become corrupted or unavailable for future use
- Once data has been entered into an LLM, almost impossible to delete it from the app
- Patient consent could be unclear



©2024 Canada Health Infoway

Canada Health Infoway

Ambient Scribe Security Checklist

- Understand where the data is going and saved (locally or in the cloud)
  - Document data flows from your organization
    - Can data be saved in a private cloud while processing is with the vendor?
  - Use existing technical security controls already in place and consider new ones to add
    - Existing DLP solution, firewall (new rules around AI scribe), 2FA, intrusion detection systems, access logs, and end-to-end encryption

- Establish written policies around the use of AI scribe software
  - Who can use it and in what situations?
    - Acceptable Use Policy
    - Role based access control (RBAC)
  - Will the patient have access to the transcription?
  - Will the note adhere to applicable privacy requirements?

©2024 Canada Health Infoway

Canada Health Infoway

Ambient Scribe Security Responses

- Administrative controls:
  - Review vendor documentation around the product and their own privacy and security policies
  - Are these products off-the-shelf with a licensing agreement or through a contracted procurement process?
  - Evaluate the software as per your organization's risk tolerance levels
  - Audit schedules
  - Update response plans to reflect AI technology in use at the organization
  - Review with your IT department for shadow AI
  - Have a person designated at your organization who can be accountable and responsible for AI

- Legislation and regulation in this area continues to evolve
  - Technology tends to outpace regulation

©2024 Canada Health Infoway

Canada Health Infoway

Canada Health Infoway

Questions & Comments

Perry Kjargaard
Senior Director
Canada Health Infoway

Robert Martin
Senior Director
Canada Health Infoway