Health Privacy on the Board Agenda: Privacy Considerations and Trends in the Health Sector

Nicole Minutti

Senior Health Policy Advisor

Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Manitoulin Health Centre
Board of Directors

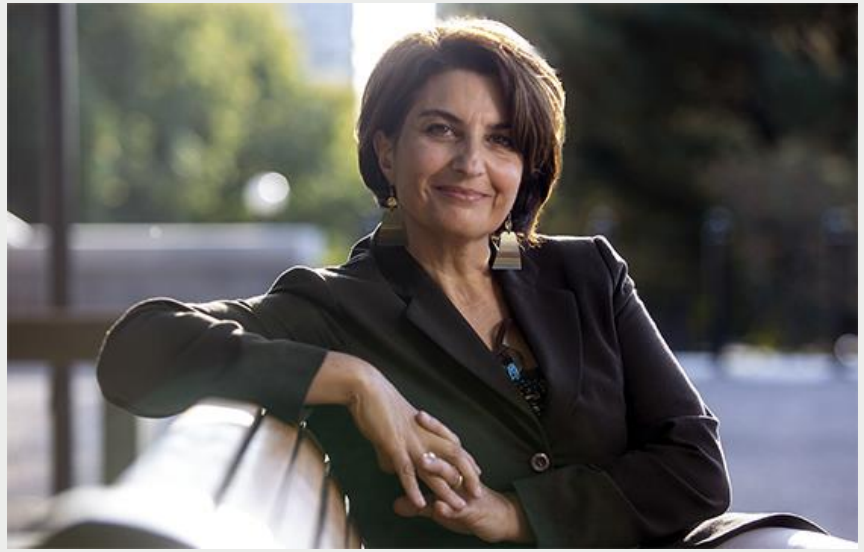
Jan 25, 2023

Agenda

- About the IPC
- Application of FIPPA and PHIPA to Hospitals
- Best Practices from PHIPA Decisions
- Best Practices from the PP/PE Manual
- Health Privacy Trends in Ontario

The Office of the Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario



Patricia Kosseim

- Ontario's Information and Privacy Commissioner is an officer of the legislature
  - Appointed by and reports to the Legislative Assembly of Ontario
  - Independent of the government of the day
- The IPC has authority under the following laws:
  - *Freedom of Information and Protection of Privacy Act* (FIPPA)
  - *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)
  - *Personal Health Information Protection Act, 2004* (PHIPA)
  - *Child, Youth and Family Services Act, 2017* (CYFSA)
  - *Anti-Racism Act, 2017* (ARA)
  - *Coroners Act*

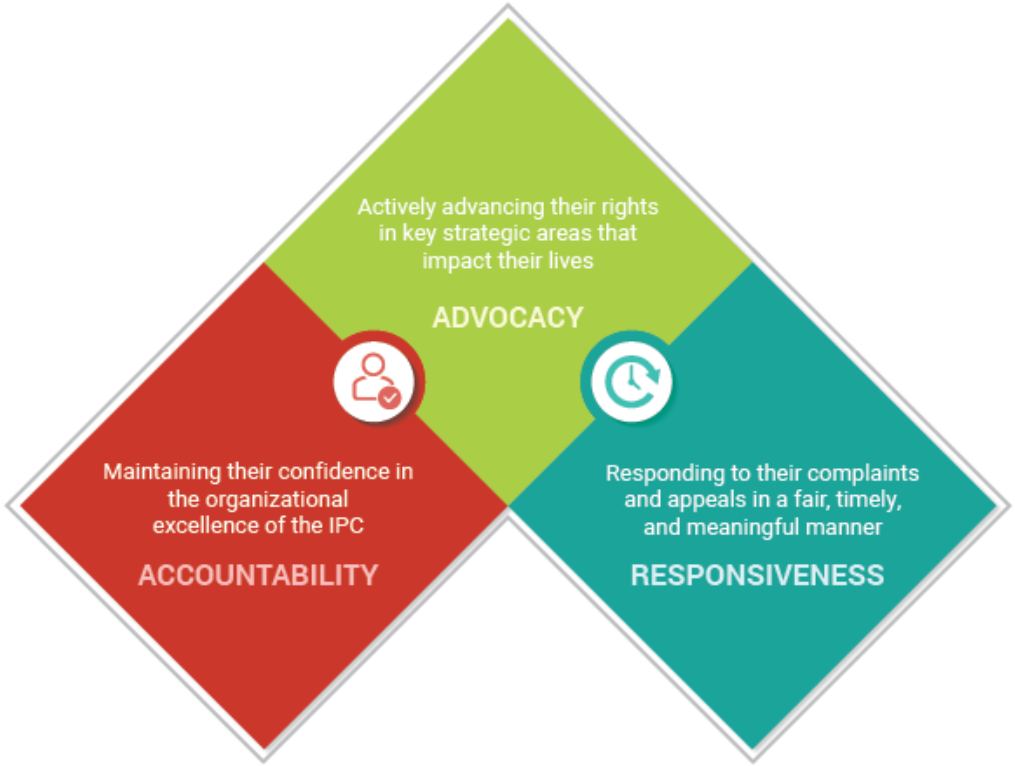
IPC's Overall Role & Mandate

In addition to overseeing provincial access and privacy laws, the office of the IPC also serves the government, public institutions and the public through its mandate to:

- Resolve appeals when access to information is refused
- Investigate privacy complaints related to personal information
- Ensure compliance with the province's access and privacy laws
- Review privacy policies and information management practices
- Conduct research on access and privacy issues and provide comment on proposed legislation and government programs
- Educate the public, media and other stakeholders about Ontario's access and privacy laws and current issues affecting access and privacy

IPC'S VISION

Enhance Ontarians' trust that their access and privacy rights will be respected by ...



IPC's Role in the Health Sector

- Issue access and privacy decisions
- Provide review and comment on health sector organization policies
- Provide guidance for health information custodians (and beyond)
- Conduct research on access and privacy issues relevant to the health sector
- Provide presentations and participate in consultations with health sector
- Consult with government regarding proposed legislation and regulation
- Conduct 3-year reviews of prescribed entities, persons, and organizations
- Consult with Ontario Health regarding interoperability standards

Application of FIPPA and PHIPA to Hospitals

Privacy Law in Ontario

	Federal Public Sector	Private Sector	Ontario Public Sector	Ontario Health Sector
Generally applicable to	Government of Canada • E.g. federal ministries, agencies, crown corporations	Private sector businesses in Canada	Public sector in Ontario • E.g. government, ministries, agencies, hospitals, universities, cities, police, schools	Health care sector in Ontario • individuals, custodians (e.g. hospitals, clinics, pharmacies, etc.)
Laws (non-exhaustive)	• Privacy Act • Access to Information Act	• Personal Information Protection and Electronic Documents Act (PIPEDA) • Canada's Anti-Spam Legislation (CASL)	• Freedom of Information and Protection of Privacy Act (FIPPA) • Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)	• Personal Health Information Protection Act (PHIPA)
Oversight	• Privacy Commissioner of Canada • Information Commissioner of Canada	• Privacy Commissioner of Canada	• Information and Privacy Commissioner of Ontario	• Information and Privacy Commissioner of Ontario

FIPPA and Hospitals

- Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA) applies to Ontario's provincial ministries and most provincial agencies, boards and commissions, as well as community colleges, universities, and hospitals.
- FIPPA requires institutions to protect the privacy of an individual's personal information existing in government records.
- Individuals have a right to request access to government-held information, including general records and records containing their own personal information.
- FIPPA sets out the obligations of the "head" of the institutions.
  - In the case of hospitals, the head is the Chair of the Board of Directors.
  - The head's powers and duties may be delegated; however, the head remains accountable.

PHIPA and Hospitals

- Ontario's *Personal Health Information Protection Act, 2004* (PHIPA) sets out rules for the collection, use and disclosure of personal health information (PHI) by health information custodians (custodians).
- Hospitals are custodians under PHIPA.
- PHIPA balances the privacy rights of individuals with the need for custodians to collect, use and disclose PHI to deliver effective and timely health care and to plan and manage our publicly funded health system.
- PHIPA provides individuals with a right to access and request correction of their personal health information.

Hospitals: FIPPA Institutions and PHIPA Custodians

- Hospitals are both institutions under FIPPA and custodians under PHIPA.
- Generally, custodians under PHIPA who are also FIPPA institutions are governed by PHIPA, not FIPPA with respect to the PHI in their custody or control, with some exceptions, for example:
  - Required disclosure
    - Public interest override
  - Permitted disclosures
    - For a consistent purpose
    - To law enforcement to aid in an investigation
    - To the Government of Canada to facilitate auditing of shared cost programs

FIPPA: Exemptions from Disclosures

FIPPA includes some mandatory and discretionary exemptions to disclosure that apply to hospitals as FIPPA institutions, for example:

- Mandatory exemptions
  - Cabinet records
  - Trade secrets (“third-party exemption”)
- Discretionary exemptions
  - Intergovernmental relations (including Indigenous communities) when received in confidence
  - Advice or recommendations within the institution
  - Law enforcement
  - Information that could endanger the health or safety of an individual
  - Information already available to the public or soon to be published

Annual Statistical Reporting Under FIPPA

- FIPPA institutions are required to provide annual reports to the IPC
- The information in the reports include, for example:
  - The number of access requests received,
  - The number of requests refused,
  - The number of appeals commenced,
  - The number of times personal information was used or disclosed for a purpose which is not included in the institution's statements of uses and purposes,
  - The amount of fees collected, and
  - Any other information showing the institution's effort to implement the purposes of FIPPA.
- A summary and more detailed statistical information is made available through the IPC's annual reports.

Annual Breach Reporting Under PHIPA

- Custodians under PHIPA must submit breach statistics to the IPC every year where information was:
  - Stolen
  - Lost
  - Used without authority
  - Disclosed without authority
- A summary and more detailed statistical information is made available through the IPC's annual reports.

Point-in-Time Breach Reporting Under PHIPA

- Custodians under PHIPA must notify the IPC of the following types of privacy breaches as they happen:
  - Use or disclosure without authorization
  - Stolen information
  - Further use or disclosure without authority after a breach
  - Pattern of similar breaches
  - Breaches related to a disciplinary action against a college or non-college member
  - Significant breaches
- Point-in-time reporting is generally not required when a breach is:
  - Not intentional
  - A one-off incident
  - Not part of a pattern
- All breaches, including those that did not meet the threshold for point-in-time reporting, must be included in the custodian's annual statistical report.

Notice to Regulatory Colleges (Under PHIPA)

- Custodians are required to notify a health care practitioner's regulatory college within 30 days if a practitioner:
  - Was an employee or agent of the custodian and was terminated, suspended, or subject to disciplinary action due to a breach.
  - Had their privileges or affiliation revoked, suspended, or restricted due to a breach.
  - Resigns and the custodian has reason to believe that the resignation is related to an investigation or other action carried out due to an alleged breach.
  - Relinquishes or voluntarily restricts their privileges or affiliation and the custodian has reasonable grounds to believe that it is related to an investigation or other action carried out due to an alleged breach.

Notice to Affected Individuals

- Custodians are required to notify affected individuals at the first reasonable opportunity if PHI is stolen, lost or accessed by an unauthorized person.
- There are many factors to consider when deciding on the best form of notification (e.g., the sensitivity of the PHI).
- The following information should be provided:
  - Name of the agent responsible for the unauthorized access, where appropriate
  - Date of the breach
  - Description of the nature and scope of the breach
  - Description of the PHI that was subject to the breach
  - Measures implemented to contain the breach, and
  - Name and contact information of the person in your organization who can address inquiries.
- Notice to affected individuals must include a statement letting them know they are entitled to make a complaint to the IPC.

Examples of Best Practices for Health Sector Boards: *PHIPA Decisions*

Individuals May Have a Right of Access to Board Meeting Minutes Where they Contain PHI

- In PHIPA Decision 17 (2015), an individual requested access to records relating to the birth and death of his infant child and the care given to his wife and child at the hospital. He also requested access to records related to himself.
- In this case, the IPC found that records such as correspondence between a hospital and its lawyers and minutes of hospital board meetings qualified as records of PHI because they contained information that arose from, and were referable to, the provision of health care to the patient at the hospital.

Boards Should Ensure Legal Authorities Are Formally Agreed Upon in Multi-Party Settings

- In PHIPA Decision 62 (2017), a physician accessed records of PHI without authorization.
- Two organizations that were co-located in the same building and providing multidisciplinary health care to the same patients, with one organization providing EMR access to the other, had no formal relationships established between them.
- Both organizations submitted that they were custodians of the PHI at issue.
- The lack of formal arrangements and identification of the custodian meant that there was no clear entity with the authority to require privacy training of all personnel who had access to the EMR, or to discipline staff and professionals in a meaningful way with respect to non-compliance with privacy breaches.
- The organizations subsequently entered into a formal agreement that was approved by the boards of both organizations.

Timing of Board Meetings Should Not Delay Production of Documentation

- In PHIPA Decision 114 (2020), the custodian did not meet a deadline imposed by the IPC to produce certain documentation in support of the IPC's breach investigation due to approvals needed from executives and a special committee of the board.
- Under PHIPA, the IPC is permitted to demand the production of any records or documents when conducting a review of a potential contravention of PHIPA.
- Custodians have an obligation to provide whatever assistance is reasonably necessary, including using any data storage, processing or retrieval device or system to produce a record in readable form, if the demand is for a document.
- The custodian was issued an interim order to perform its duty to assist the IPC with its review of the breach.

Timing of Board Meetings Should Not Delay Breach Notification

- In PHIPA Decision 210 (2023), there was a cybersecurity attack that resulted in a breach of PHI at a hospital.
- It took four months for the hospital to notify affected individuals.
- Notification was delayed due to a postponement of a board meeting.
- The adjudicator found this was not a valid reason for delay and that, given the magnitude and seriousness of the breach, a board meeting should have been specially convened to approve the public notice much sooner.

Examples of Best Practices for Health Sector Boards: *The Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*

The Manual for the Review and Approval of Prescribed Persons and Prescribed Entities

- Custodians may disclose PHI without consent to prescribed persons (PPs) to compile or maintain registries of PHI, for example, to facilitate or improve the provision of health care.
- Custodians may also disclose PHI without consent to prescribed entities (PEs) for the purpose of analysis or compiling statistical information with respect to the planning, management, evaluation, and monitoring of the health system.
- One of the conditions for this disclosure of PHI to be made without consent is that PPs and PEs have their practices and procedures reviewed and approved by the IPC every three years.
- The *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* sets out the requirements that are reasonably necessary to protect the PHI that PPs and PEs are permitted to collect.

Governance and Accountability Frameworks

- The Manual requires that PPs and PEs establish privacy and security governance and accountability frameworks for ensuring compliance with PHIPA and its regulations as well as the policies, procedures and practices implemented by the organization.
- The Manual outlines the minimum requirements for these frameworks, including that they:
  - Describe role of the board in respect of the privacy and information security programs, including any committee of the board with privacy oversight.
  - Address the frequency that the board will be updated with respect to the privacy and information security programs, which should be at least annually, and preferably in the form of a written report.

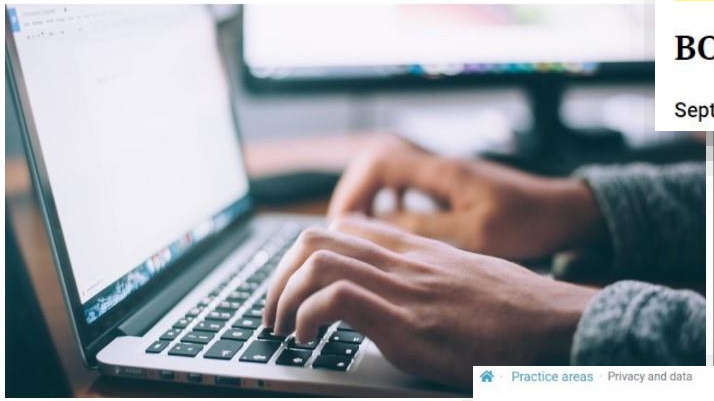
Privacy and Information Security Reporting to the Board

- The update provided to the board of directors must, at a minimum, address risks that may negatively affect the PP's or PE's ability to protect PHI that have been ranked as "high risk" on the corporate risk register.
- Such matters should include, for example:
  - Major financial investments required to ensure robust and sustainable privacy and information security governance and accountability frameworks
  - Regular updates on the level of cybersecurity risks facing the organization and the mitigation measures
  - Major IT transformation projects with privacy implications (e.g. artificial intelligence)
  - Findings, mitigations and any other relevant recommendations arising from privacy audits and PIAs
  - Findings and recommendations arising from information security audits (e.g. TRAs)
  - Privacy breaches, suspected privacy breaches, and privacy complaints, including the findings, mitigations, and any other relevant recommendations arising from their investigations
  - Information security breaches, including the findings, mitigations, and other relevant recommendations arising from these investigations

Health Privacy Trends in Ontario

Trend: Cybersecurity Attacks

Perinatal and child registry data breach affects health info of 3 million Ontarians



An Ontario agency that collects data on pregnancies and births in the province says a resulted in a leak of personal health information of approximately 3.4 million people.

By Tyler Griffin, The Canadian Press
Posted September 25, 2023 1:55 pm. Last Updated September 25, 2023 1:58 p

PRIVACY & SECURITY

BORN agency suffers cybersecurity attack

September 27, 2023

Canadian organizations averaged 25 cybersecurity incidents in the past year, finds EY survey

Français

Practice areas · Privacy and data

Cybersecurity incident protection becoming prohibitively expensive as threats multiply, says

News / Local News

Five Southwestern Ontario hospitals scramble after cyberattack disruption

Five Southwestern Ontario hospital were scrambling to notify and accomm provider wor

Paul Morden

Published Oct 24, 20

Windsor

Cyberattack at 5 southwestern Ontario hospitals leaves patients awaiting care

The attack on 5

CBC News · Posted:

ARE THIS ARTICLE

en attacks occur

Local News

Stolen cyberattack data includes info on every Sarnia hospital patient in last 30 years

Trevor Wilhelm

Published Nov 09, 2023 • La

News / Local News

Do more to protect patient data from cybercriminals: IT experts

Hospitals are a "treasure trove" of highly sensitive personal data that can be used for extortion, making them an ideal target for cyberattacks, says an IT expert

GTA

Michael Garron Hospital ransomware attack compromised personal data of employees, clinicians

nce numbers, bank account numbers and earnings

News / Local News

Southwestern Ontario hospitals confirm theft of millions of records in cyberattack

The hackers behind an ongoing cyberattack against five Southwestern Ontario hospitals stole personal details from close to 300,000 people — including more than 5.6 million records from one facility alone.

Trevor Wilhelm

Published Nov 06, 2023 • Last updated Nov 06, 2023 • 5 minute read

PRIVACY & SECURITY

Cyber-thieves put hospital data on dark web

November 8, 2023

Spark

Paying ransom for data stolen in cyberattack bankrolls further crime, experts caution

Ceding to demands can alert other hackers, with no guarantee access will be granted

Jason Vermes · CBC Radio · Posted: Nov 18, 2023 4:00 AM EST | Last Updated: November 18

News / National

Hackers demanded multimillion-dollar ransom to end attack against Ontario hospitals

But even after the hackers started posting millions of patient files online, the hospitals and their shared service provider refused to pay the ransom.

Trevor Wilhelm

Published Nov 16, 2023 • Last updated 1 week ago • 3 minute read

For the first time, top leadership from the five southwestern Ontario hospitals hit by a ransomware attack answered questions from the media — acknowledging the significant impact the incident has had on care, as well as the large amount of stolen data.

During the roughly 50-minute meeting on Friday, each hospital CEO said their facility has been hard hit by the Oct. 23 attack, but recovery is ongoing and they're getting by with the hard work of staff. With systems down and hospitals unable to access critical information, thousands of patient appointments have been cancelled across the five hospitals, creating backlogs of varying lengths at some of the facilities.

Cybersecurity Attack Trends

- The number and types of attacks are increasing
  - Last year, the Canadian Centre for Cybersecurity blocked up to 5 billion attempts on Government of Canada systems *per day*
  - Tactics are no longer limited to locking down information; now usually include threats to expose sensitive information
- Victims are increasingly including public institutions; hospitals are a common target
- Bigger payouts: the average ransom paid in Canada in 2022 was over $250,000
- Lower bar for entry: it's easier than ever to be a cyber criminal
- Pandemic and movement to work-from home has expanded the "threat surface"
- "Collective defense" is being explored in the health sector

PRIVACY & SECURITY

Report: Cyber attack attempts increased 104% in 2023

January 24, 2024

SAN FRANCISCO – Armis, the asset intelligence cybersecurity company, today announced, The Anatomy of Cybersecurity: A Dissection of 2023's Attack Landscape. The 2023 analysis of Armis' proprietary data offers critical insight into the multifaceted challenges global organizations face when it comes to protecting the entire attack surface. Report findings serve as a blueprint to help security teams worldwide prioritize efforts to reduce cyber risk exposure in 2024.

The report found that global attack attempts more than doubled in 2023, increasing 104%. Utilities (over 200% increase) and Manufacturing (165% increase) were the most at risk industries. Attack attempts peaked in July, with communications devices, imaging devices and manufacturing devices experiencing intensified targeting during this period.

"Armis found that not only are attack attempts increasing, but cybersecurity blind spots and critical vulnerabilities are worsening, painting prime targets for malicious actors," said Nadir Izrael (pictured), CTO and co-founder, Armis. "It's critical that security teams leverage similar intelligence defensively so that they know where to prioritize efforts and fill these gaps to mitigate risk. We hope that by sharing these insights, global businesses and governments will leverage them to immediately pinpoint what they should be focusing on to improve their cybersecurity posture this year to keep critical infrastructure, economies and society safe and secure."

Report: Cyber attack attempts increased 104% in 2023 | Canadian Healthcare Technology (canhealth.com)

PHIPA Decisions Related to Cybersecurity Attacks

- Decision 210: Cyberattack on a public hospital
  - Several hospital systems were accessed through a password-spraying attack that compromised a privileged account
  - Concerns about account privileges, system protections, strength of passwords, and notification timelines
- Cyberattack on laboratory system
  - The IPC undertook a joint investigation with the IPC in BC which found that the company failed to implement reasonable safeguards to protect the PHI of millions of Canadians
  - Jointly, the IPC in Ontario and BC ordered the organization to:
    - Improve specific practices regarding information technology security
    - Formally put in place written information practices and policies with respect to information technology security
    - Cease collecting specified information and to securely dispose of the records of that information which it has collected
  - The Ontario IPC issued the following additional orders:
    - To improve its process for notifying individuals
    - To clarify and formalize its status with respect to the custodians in Ontario with whom it has contracts

Lessons for Boards

- Keep abreast of best practices identified by regulators and cybersecurity experts
  - For example, the PP/PE Manual recommends that boards receive regular updates on the level of cybersecurity risks facing the organization and the mitigation measures
- "An ounce of prevention is worth a pound of cure" – invest in the prevention of cybersecurity attacks (e.g. training, infrastructure, etc.)
- Have plans in place for how to mitigate and remediate a cybersecurity attack well in advance of their occurrence
- Keep up-to-date on the changing landscape for cybersecurity insurance
- Consider whether collective defense is an appropriate option for your organization

IPC Resources

Unmasking Digital Threats: How to Guard Against Cyber Crime (Podcast)

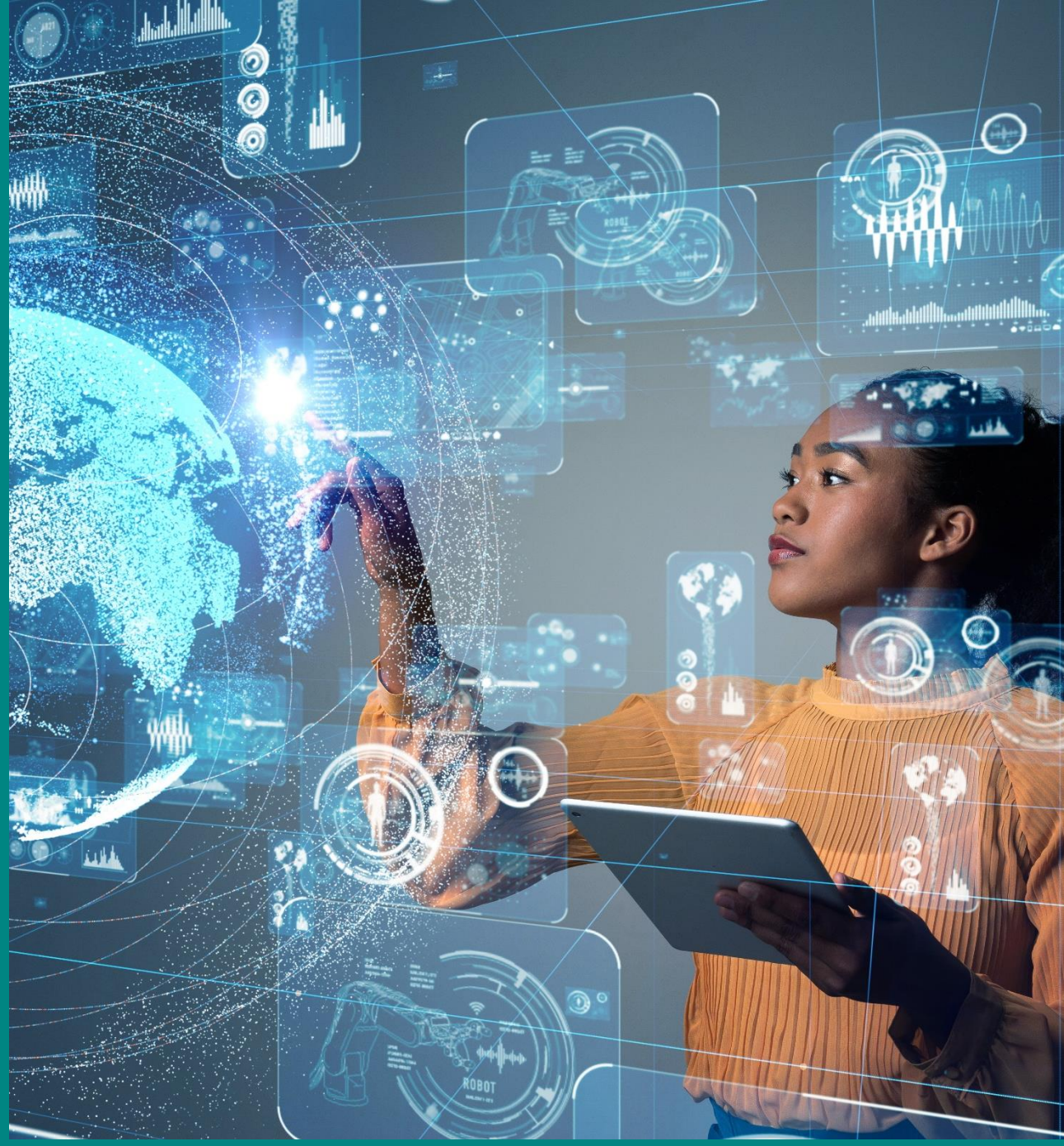
Detecting and Deterring Unauthorized Access to PHI (Guidance)

How to Protect Against Ransomware (Technology Fact Sheet)

Responding to a Health Privacy Breach: Guidelines for the Health Sector (Guidance)

Protect Against Phishing (Technology Fact Sheet)

Trend: Artificial Intelligence



NEXT GEN INVESTING

‘Godfather of AI,’ ex-Google researcher: AI might ‘escape control’ by rewriting its own code to modify itself

Published Wed, Oct 11 2023•8:30 AM EDT

Tom Huddlest

ARTIFICIAL INTELLIGENCE

AI and the Ascendancy of Non-Physician Providers

The evolution of care must include human and technological elements.

Posted September 21, 2023 | Reviewed by Ray Parker

Alberta Innovates is looking to enable better health through artificial intelligence

ARTIFICIAL INTELLIGENCE

Chatbots: The Future of Healthcare

Medical chatbots can encourage people to sooner.

Posted September 27, 2023 | Reviewed by Davia Sills

Thanks to generative AI, profits are up and costs are down at these businesses

Generative AI has already started to save companies millions, upending workflows, changing hiring plans and shifting investment criteria. And the enthusiasm shows , despite the caution signs

LOGY REPORTER

Local News

Artificial intelligence promises to change the way health care works

Get the latest from Elizabeth Payne straight to your inbox

Sign Up >

Elizabeth Payne

Published Sep 26, 2023 • Last updated Oct 02, 2023 • 5 minute read

AI-powered tool to streamline care in emergency departments receives $1.5M in funding

September 27, 2023

Microsoft launches new AI services for Health

AI Will Help Bridge Gaps in Canadian Healthcare

October 4, 2023 Colin Hung 3 Min Read

ARTIFICIAL INTELLIGENCE, DEMOCRACY, SECURITY

Canada Needs an Artificial Intelligence Agency

Generative AI applications are just the tip of the iceberg.

Dan Ciuriak, Anna Artyushina

October 5, 2023

Damian Jankowicz moves crosstown to Unity Health

November 1, 2023

TORONTO – Damian Jankowicz (pictured) joine an executive vice president and its first chief inf Health, he will steward major technological tran implements a new electronic patient record thr grow its cutting-edge AI team.

TORONTO | News

Toronto hospital network appoints chief AI scientist in bid to improve health care

Big changes on the way: Doctors say AI will improve health care

Artificial intelligence technology is already being used in Ontario to predict the future health of people based on existing health data

PEI

AI will be critical for the future of rural health care in Canada, experts say

Fewer specialists, doctors, nurses in rural Canada means AI will play a larger role

Cody MacKay · CBC News · Posted: Oct 15, 2023 6:00 AM EDT | Last Updated: October 16

Artificial Intelligence: Ethical and Privacy Concerns

- AI technologies make it possible to process tremendous amounts of personal data; in the case of generative AI, algorithms can be used to create entirely new content.
- These technologies raise serious ethical and privacy concerns, while also offering beneficial uses in certain situations.
- AI technologies, and generative AI in particular, have the potential to create damaging content that can sustain unfair biases and put privacy and other fundamental human rights at risk.
- Strong legal and ethical safeguards are needed to ensure that AI technologies are used in an accountable, transparent, and ethically responsible manner that fosters public trust.

AI in the Health Sector Trends

- Federal government
  - Bill C-27, the Digital Charter Implementation Act
  - The Artificial Intelligence and Data Act (AIDA) Companion Document
  - Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems
  - Health Canada draft guidance: "Pre-market guidance for machine learning-enabled medical devices"
  - Guidance for the responsible use of AI by government
- Provincial governments
  - Ontario's Trustworthy AI Framework (IPC Ontario Comments)
- Regulators
  - Joint statement on the use of AI technologies (Ontario IPC and Ontario Human Rights Commission)
  - Joint special report "Getting Ahead of the Curve" (BC and Yukon)
  - Ontario IPC joined international regulators in co-sponsoring two resolutions on AI
  - Ontario IPC participates with federal, provincial, and territorial counterparts to develop joint resolutions including "Principles for Responsible, Trustworthy and Privacy-Protective Generative AI Technologies"
- **Health sector organizations** are implementing AI solutions; creating AI-related positions
- **Educators** are offering an increasing number of AI-related courses, certificates and degree programs

Lessons for Boards

- Keep abreast of best practices identified by regulators and health sector AI experts
  - For example, the PP/PE Manual recommends that boards receive regular updates on major IT transformation projects with privacy implications (e.g. artificial intelligence)
- Keep up-to-date on changing legislation
- Three overarching questions boards should be asking of major AI proposals:
  - “May we do it?” (legal question)
  - “Can we do it?” (technical, financial, feasibility question)
  - “Should we do it?” (ethical question)

Conclusion

Additional Resources

FIPPA

Ontario's Freedom of Information and Protection of Privacy Act: A Mini Guide

FAQ: Statistical Report of FIPPA/MFIPPA Institutions

PHIPA

A Guide to the Personal Health Information Protection Act

Frequently Asked Questions: Personal Health Information Protection Act

PHIPA and FIPPA Institutions

Freedom of Information at Hospitals: Frequently Asked Questions

Fact Sheet: Applying PHIPA and FIPPA/MFIPPA to Personal Health Information

Breach Reporting

Annual Reporting of Privacy Breach Statistics to the Commissioner

Reporting a Privacy Breach to the IPC: Guidelines for the Health Sector

Responding to a Health Privacy Breach: Guidelines for the Health Sector

Contact Us

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

TDD/TTY: 416-325-7539

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

Media: media@ipc.on.ca / 416-326-3965