



# ***PRIVACY & SECURITY***

**+**

# ***YOUR EMR***

**Ariane Siegel**

**General Counsel & Chief Privacy  
Officer**



# Your Presenter: Disclosure

**Presenter: Ariane Siegel**

**General Counsel & Chief Privacy Officer,  
OntarioMD**

- **No Relationship with Commercial Interests**
- **No Financial Support**
  - This program has not received financial support or in-kind support from any organization
- **No Conflict of Interest**
  - Ariane Siegel has not received payment or funding from any organization supporting this program AND/OR organization(s) whose product(s) are being discussed in this program
- **No Bias**
  - There are no potential sources of bias



# Outline

---

- 1. The Role of OntarioMD**
- 2. The Privacy Landscape: Basics**
- 3. Compliance/PHIPA**
- 4. Governance**
- 5. The EMR Dashboard**
- 6. Privacy Breach**
- 7. Accountability**
- 8. What you can do**
- 9. Important Decisions by the IPC**
- 10. The Future**





# *The Role of OntarioMD*



# OntarioMD & PHIPA

---

- OntarioMD is a “Health Information Network Provider”
  - HINP because we deliver PHI via HRM.
- In relation to HICs, OntarioMD acts as an “agent”
  - We support them in their use & adoption of technology

**Mission:** OntarioMD is looking for ways to make *privacy & security* more accessible

- By developing tools/software to make privacy & security more intuitive;
- By reaching out to partners & stakeholders – the CMPA, IPC, eHealth Ontario – to develop collaborative, community-oriented privacy & security policies/tools

OntarioMD has been very successful in supporting physicians in the selection, implementation and adoption of EMRs.



# OntarioMD Products and Services



HEALTH  
REPORT MANAGER



EMR QUALITY  
DASHBOARD



PRIVACY  
TRAINING AND RESOURCES



EMR CERTIFICATION  
PROGRAM



VENDOR COLLABORATION  
PORTAL



EMR: EVERY STEP  
CONFERENCE



CLIENT SERVICES  
AND ENGAGEMENT



PEER LEADER  
PROGRAM



EMR PRACTICE  
ENHANCEMENT PROGRAM



EMR PROGRESS  
ASSESSMENT TOOL



ONTARIOMD  
REPORTS



ON THE ROAD  
WITH ONTARIOMD



# OntarioMD Partners and Partnered Initiatives

## Partners:



## Partnered Initiatives:



eCONSULT DEPLOYMENT  
AND EMR INTEGRATION



eREFERRAL



eNOTIFICATIONS



OLIS  
DEPLOYMENT



DIGITAL HEALTH  
SERVICES BUNDLE

**eHealth Ontario** ONE ID

**eHealth Ontario** ONE Mail

**eHealth Ontario** ConnectingOntario



## DATA GOVERNANCE

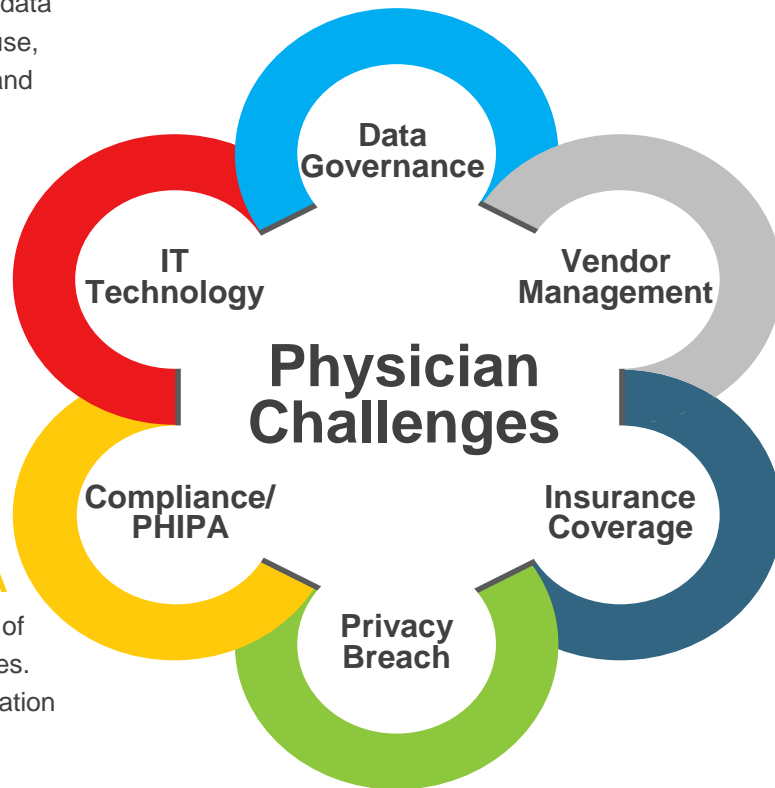
Issues related to data deletion, data ownership, data storage, data use, data portability, data retention and data migration.

## IT TECHNOLOGY

Management, adoption and implementation of new technologies.

## COMPLIANCE/PHIPA

Understanding the implications of the law, & HIC signing authorities. New IPC rules regarding notification of Privacy Breaches.



## PRIVACY BREACH

Ransomware and Response Plan.

## INSURANCE COVERAGE

Concerns over medical-legal risk, legal defence, liability protection, cyber liability & risk- management protection.

## VENDOR MANAGEMENT

Costs, dispute resolution, warehousing, standards, and privacy.





# Critical Concerns for Health Care

---

- **Privacy law is a rapidly developing & increasingly litigious area**
- **Data breaches have become more frequent**
- **Technology is deeply integrated into the Health Care System**
- **Responsible data handling is fundamental to patient care & the health care profession**





**KEEP  
CALM  
I'M A  
LAWYER**



# COMPLIANCE/ PHIPA

## *The Privacy Landscape: Basics*



# Privacy: Complexities & the Law

---

- Doctor-patient relationship is governed by complex legislation & confidentiality requirements
- The demands to preserve privacy & confidentiality are complicated by pressure for:
  - Better health information sharing
  - Increased efficiency of health care



COMPLIANCE/  
PHIPA



EMR: EVERY STEP  
CONFERENCE

#OMDESC18

OntarioMD  
Empowered Practices. Enhanced Care.

# Relevant Legislation & Regulations

## PRIVACY

- PIPEDA (FEDERAL)
- PHIPA
- FIPPA
- COMMON LAW
- CONTRACTS/UNION
- TORTS-INTRUSION UPON SECLUSION
- CRIMINAL CODE

COMPLIANCE/  
PHIPA

## OTHER

- MEDICINE ACT
- CPSO GUIDELINES
- COURT ORDERS



# *Personal Health Information Protection Act*

“*PHIPA*” has stood as the statutory framework for collection, use, & disclosure of PHI since 2004.

- “Health Information Custodians” (HIC) under *PHIPA* = physicians & healthcare providers



## Key Principles:

- Physician-patient relationship is built on trust
- ‘Consent-based’ legislation

COMPLIANCE/

PHIPA



EMR: EVERY STEP  
CONFERENCE

#OMDESC18

OntarioMD  
Empowered Practices. Enhanced Care.

# Amendments to *PHIPA*

## As of October 1, 2017:

- Under Section 12(2), requirement for HICs to *explicitly notify* individuals that they are entitled to report the theft, loss, unauthorized use, or disclosure of their personal information to the **Information & Privacy Commissioner (IPC)**
- Obligations for HICs to report to **IPC**, based on seven expanded criteria
- Report statistics to IPC
- ‘Privacy Breach Report Form’ on website for HICs to complete

COMPLIANCE/  
PHIPA



EMR: EVERY STEP  
CONFERENCE

#OMDESC18



Information and  
Privacy Commissioner  
Ontario, Canada

OntarioMD  
Empowered Practices. Enhanced Care.



# *Consent: The Building Block of Privacy Law*

COMPLIANCE/  
PHIPA

---

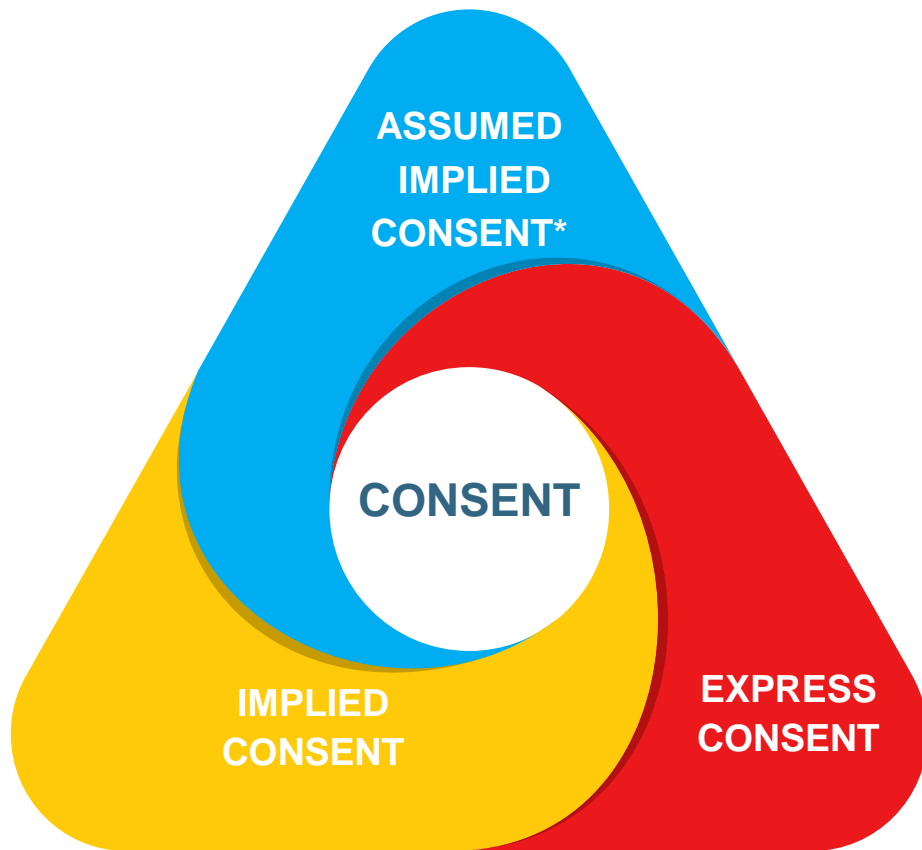


EMR: EVERY STEP  
CONFERENCE

#OMDESC18

OntarioMD  
Empowered Practices. Enhanced Care.





**\*unless express consent is explicitly required by PHIPA**

## Must be:

- (i) that of the individual;
- (ii) knowledgeable;
- (iii) relate to the information; &
- (iv) not be obtained through deception or coercion

COMPLIANCE/  
PHIPA



# CONSENT

EXPRESS	IMPLIED	ASSUMED IMPLIED
<p><b>Required when a HIC:</b></p> <ul style="list-style-type: none"><li>discloses PHI to a non-HIC, another HIC for a purpose other than providing health care to individual;</li><li>collects, uses or discloses PHI for marketing or market research; fundraising (if using more than name &amp; address)</li></ul>	<ul style="list-style-type: none"><li>May be relied upon whenever a HIC uses PHI for most purposes under PHIPA</li><li><b>Examples:</b><ul style="list-style-type: none"><li>➤ Having a patient attending an appointment</li><li>➤ Providing a referral to a specialist</li></ul></li></ul>	<ul style="list-style-type: none"><li>Allows a HIC to disclose PHI to another HIC within the patient's <b>circle of care</b> for healthcare purposes</li></ul>

# The Circle of Care

## 'Circle of Care'



## The 'Lock Box'



COMPLIANCE/  
PHIPA



EMR: EVERY STEP  
CONFERENCE

#OMDESC18

OntarioMD  
Empowered Practices. Enhanced Care.

**PHYSICIAN**



**CHALLENGES**



# DATA GOVERNANCE



# Who Owns the Medical Record?

---

- PHI in medical records
- Possession of medical records physicians, or the person/organization responsible for file's creation (i.e., hospital or clinic)-
- Shared Custody and Control

## The Principle:

Patients have a right content of their record --exceptions (e.g. likelihood of harm to the patient not everything-See **IPC Decision 52**)

DATA  
GOVERNANCE



# Retention & Relocation

- Physicians are responsible for retaining patient records, regardless of whether they are continuing to provide care to the respective patient(s)
  - **Adult** patients: records must be kept for **10 years** from date of last entry in record
  - Patients who are **children**: records must be kept until **10 years** after day on which patient reached or would have reached the **age of 18 years**
- Transferring custody & control of patient records is governed transfer & retention regulations



DATA  
GOVERNANCE



EMR: EVERY STEP  
CONFERENCE

#OMDESC18

# Right to Possession

---

- Physicians owe a **fiduciary** obligation to their patients – an obligation to place patients' interests ahead of their own
- This obligation extends to record keeping. Physicians must:
  - **Protect the security of patients' PHI; &**
  - **Ensure that patients' have access to their PHI**
- It is important to define who has the right to possess medical records in any physician-clinical contractual relationship





# ***Scenario:*** Records in a Shared Practice

---

## Contractual obligations may:

- Delegate responsibility for maintaining & transferring patient records;
- Govern custody & control;
- Limit access to the content of medical records;
- Control transfer & possession rights.

## Untested legal question:

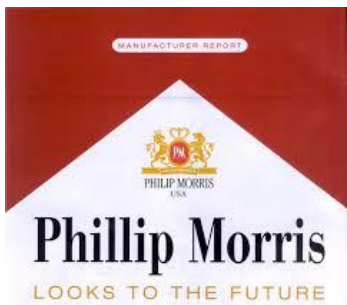
In a dispute over possession of shared, EMR-hosted records, who has the ultimate right to possession:

- The physician, or the clinic (the EMR host – through contract)?



# Secondary Use of Data

- PHI – Complicated
- De-identification of PHI and use for secondary purposes
- Unclear
- SCC Case: British Columbia v. Philip Morris International, Inc
  - Healthcare databases not compellable
  - Phillips Morris **cannot** see de-identified raw data (s.2(5)(B) of the Tobacco Damages and Health Care Costs Recovery Act)





# IT TECHNOLOGY

## *The EMR Quality Dashboard*



# What is the EMR Quality Dashboard?



IT TECHNOLOGY



EMR: EVERY STEP  
CONFERENCE

#OMDESC18

# EMR Quality Dashboard Proof of Concept

## Scope (October 2016 – December 2018)

- **Quality Dashboard Framework**
  - Real-time clinical value from provincial primary care indicators
  - Improved EMR data quality driving provincial primary care indicators
  - Scalability to create new/customized primary care indicators
- **Shared Provider Dashboard Framework**
  - Integration of a common dashboard tool to display provincial indicators
  - Collaboration among Vendors & EMRs:
    - OSCAR EMR (OSCAR 15)
    - TELUS Health (PS Suite, Med Access)



## IT TECHNOLOGY



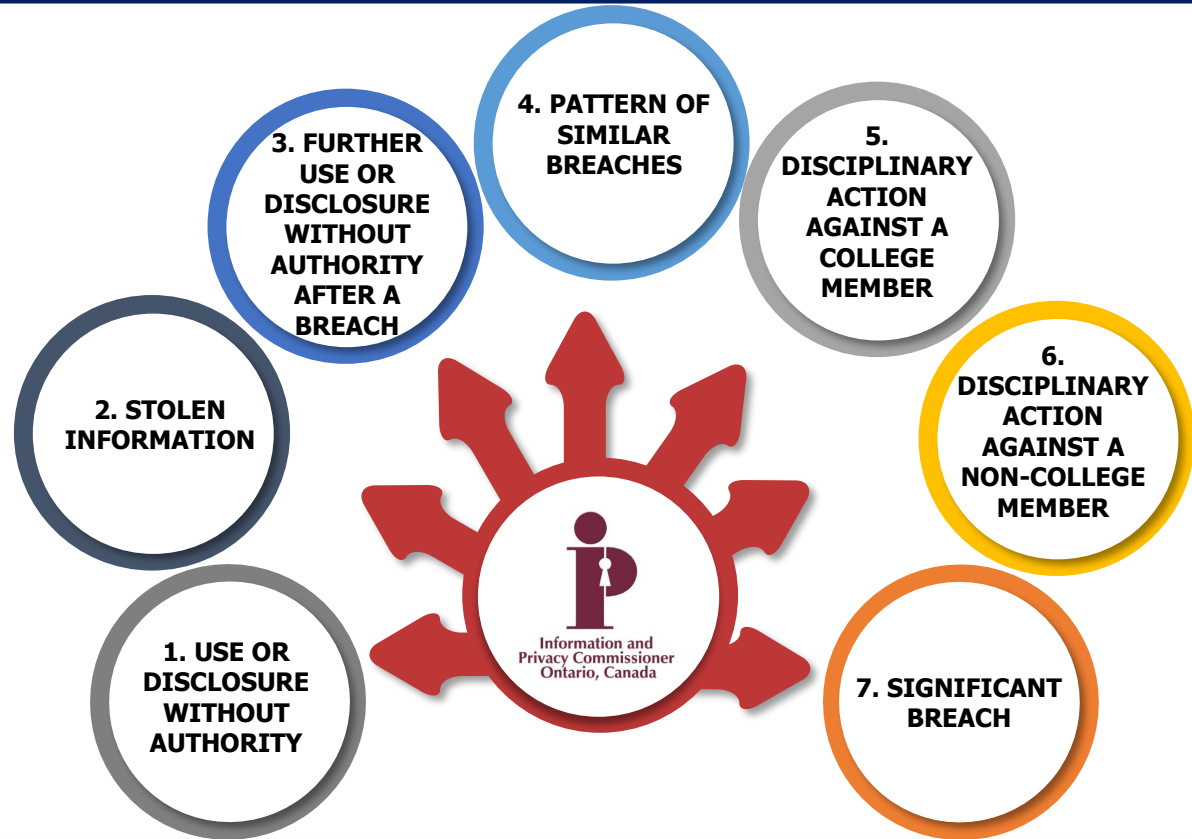
# PRIVACY BREACH



# Reporting a Privacy Breach

\*As of [October 1, 2017](#), expanded obligations for HICs to report privacy breaches.

\*Under Section 12(3), there are **SEVEN** categories that are not mutually exclusive; **more than one** can apply to a single privacy breach.



PRIVACY BREACH



EMR: EVERY STEP  
CONFERENCE

#OMDESC18

OntarioMD  
Empowered Practices. Enhanced Care.

# Privacy Breach: Ransomware

## Ransomware:

a type of malicious software designed to block access to a computer system until a sum of money is paid.



## Scenario:

May 12 - 15, 2017

*“WannaCry”* Ransomware Attack

- EMRs provide a treasure trove of PHI & PI which are extremely valuable on the black market
- BACKUP

PRIVACY BREACH



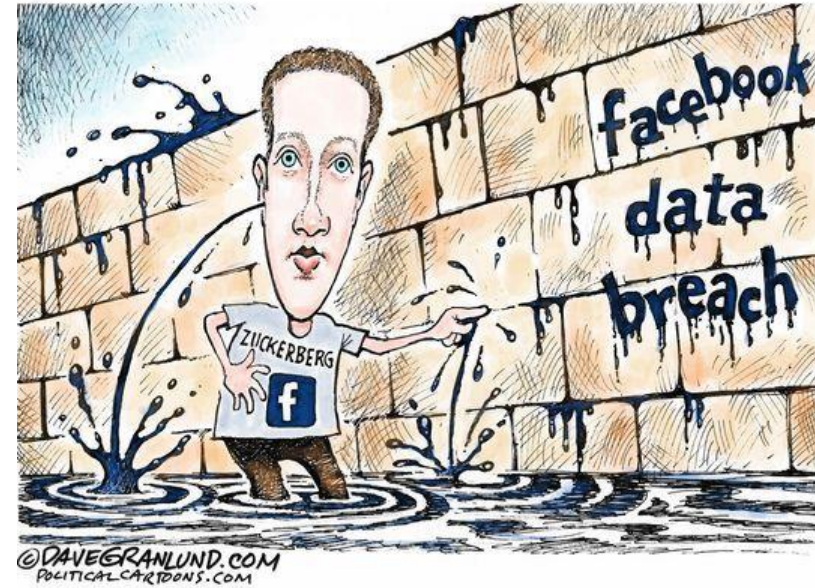
EMR: EVERY STEP  
CONFERENCE

#OMDESC18

OntarioMD  
Empowered Practices. Enhanced Care.



# Facebook to contact 87 million users affected by data breach



**Facebook's slide cost  
Mark Zuckerberg  
\$6.06 billion in one  
day**

**PRIVACY BREACH**



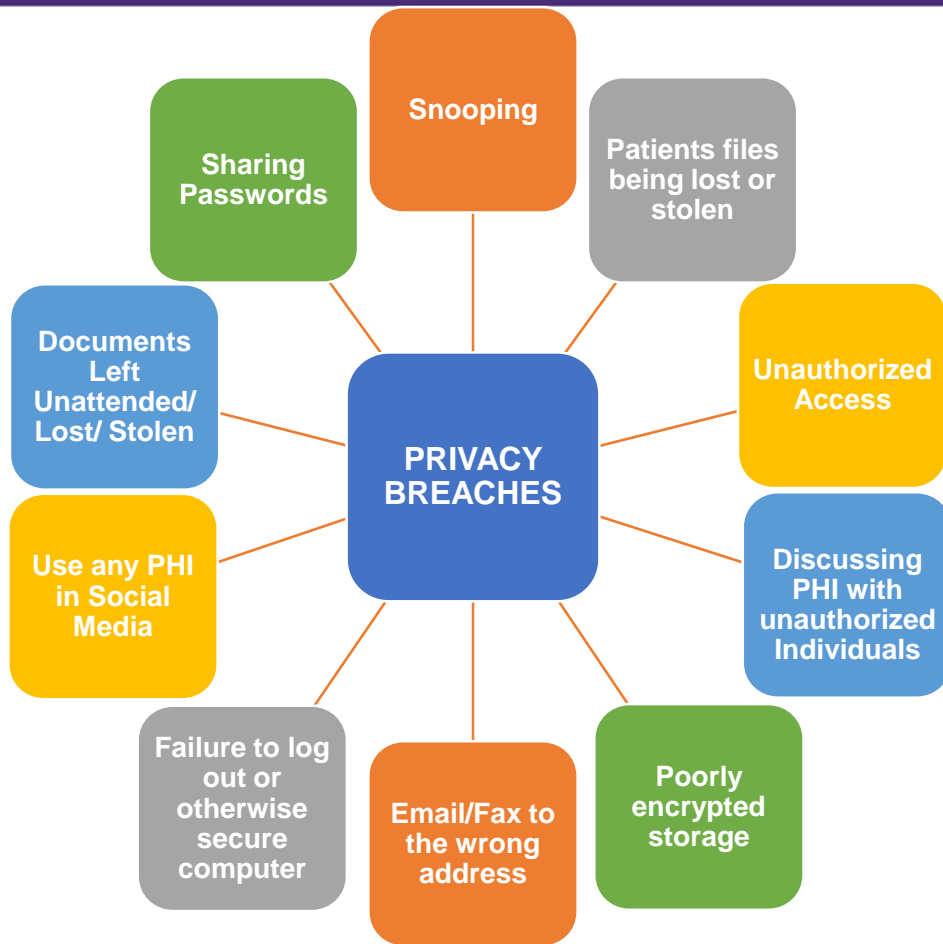
## Note:

- **Snooping:** persons accessing PHI inappropriately

Note: recent IPC disciplinary decisions have ordered fines in the 10s of 1000S of dollars to be paid by snooping clinical staff

- **Poorly encrypted storage** – unencrypted laptops, cell phones, media devices, memory sticks, CDs

Consider: the ‘internet of things’



## PRIVACY BREACH



# The Privacy Breach Management Protocol

There are **SIX** steps in the breach management process **HICs** must address:



**RESPONSE PLAN**

**CYBERLIABILITY INSURANCE**

**PRIVACY BREACH**



EMR: EVERY STEP  
CONFERENCE

#OMDESC18

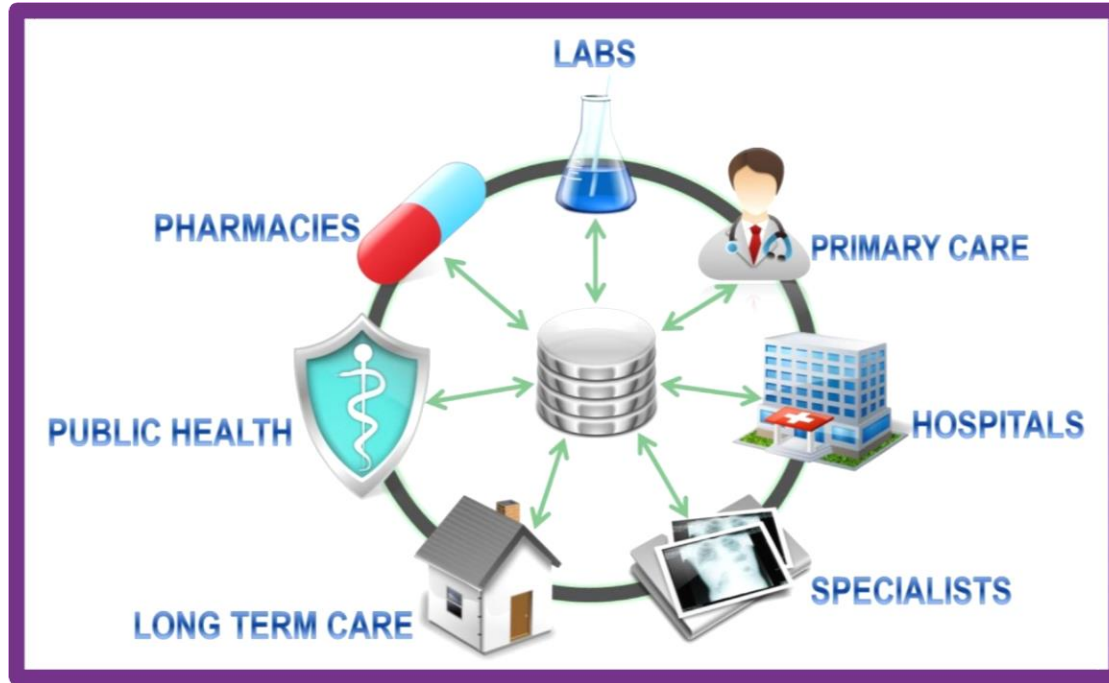
OntarioMD  
Empowered Practices. Enhanced Care.



# CREATING AN ACCOUNTABLE PRACTICE



# Accountability



## PRIVACY BREACH



EMR: EVERY STEP  
CONFERENCE

#OMDESC18

# Best Practices: Be Accountable

**Identify** responsibilities & create a structure of **accountability**

**Implement staff training** that covers the responsibilities, restrictions, confidentiality, spoofing, process for any data sharing, social media, security & privacy measures

**Follow** industry standards, best practices, & ethical standards

**Develop** prevention & breach response plans

If breach occurs: **manage** responsibly & mitigate

**Establish** audit trails with random & targeted auditing

**Limit** PHI collection to strictly necessary purposes

**PRIVACY BREACH**



# *OntarioMD's Privacy & Security Training Module*



PRIVACY  
TRAINING AND RESOURCES

PRIVACY BREACH



EMR: EVERY STEP  
CONFERENCE

#OMDESC18

OntarioMD  
Empowered Practices. Enhanced Care.

# Privacy & Security Training

- **Mission:** Create effective and practical privacy training for primary and community care
- **Goal:** Level set privacy fundamentals
- Approached by stakeholders working on rollout of the Viewer to be involved in helping design practical privacy and security training
- Project included engagement & support of **CPSO**, **CMPA**, **OMA**, & included mandatory messaging & requirements provided by **eHealth Ontario** for pilot project for onboarding the ConnectingOntario Clinical Viewer.



*eHealth Ontario*



PRIVACY BREACH



# Privacy & Security Training

---

- Currently in the process of translating the Module to French
- **Important:** IPC Decision 64 – Annual Online Privacy Training Course for its agents.
- **Privacy training program** covers a wide range of privacy-related topics:
  - purposes for which agents are permitted to collect, use & disclose PHI
  - any limitations, conditions or restrictions imposed by the hospital
  - obligations imposed on agents under PHIPA & its regulations
  - potential consequences for custodian arising from agents who collect, use or disclose PHI in contravention of PHIPA
- Currently over 500+ clinicians have completed the training

## PRIVACY BREACH

---



# How do you protect yourself & your practice?

---

- **Policies and procedures**
  - Re: privacy, system security, security incident response, and breach management, retention records, & destruction of personal information
  - Adopt OntarioMD certified EMRs – *the certification process builds in security safeguards*
- **Safeguard PHI:**
  - Use best practices to prevent loss, theft, or otherwise unauthorized access
  - Help from a Vendor/3<sup>rd</sup> Party
- **Implement Agreements:**
  - Use confidentiality agreements, contracts, information sharing agreements and service levels agreements for all providers of electronic services

PRIVACY BREACH

**\*\* Privacy has to support medical practice \*\***



# How do you protect yourself & your practice?

---

- **Implement an Association Agreement for your Practice**
  - Refer to OMA Association Agreement or OMA for advice
- **Be proactive:**
  - Actively take the necessary steps to prevent the breach from occurring
- **Train employees & representatives in all privacy & security measures:**
  - Train about acceptable use of PHI so they understand appropriate practices & policies for handling of PHI & consequences of disciplinary action that may result if they engage in improper use
- **Safeguard PHI:**
  - Use best practices to prevent loss, theft, or otherwise unauthorized access

***\*\*Don't rush. Stop and think.\*\****

## PRIVACY BREACH

---



# Implement – Security Safeguards (1)

PRIVACY BREACH

## PHYSICAL SAFEGUARDS

Firewall, encryption	Credential-based access (2 factor authentication), password protection, masking, encryption, time outs
Daily Back Up	Local and cloud
Out of public view	Away from public view, don't store devices in car, encrypted USB keys, establish secure areas, sign in and badges, server in secure area, log out
Audit Logs	Authentication, warning flags for consent directives
Anti-virus	Software - automatic updates, active firewall on networks

## ADMINISTRATIVE/PROCESS SAFEGUARDS

Confidentiality Agreement	Staff and 3 <sup>rd</sup> Parties
Patient Education	Informed consent. Implied consent for sharing within circle of care. Record of consent
Staff Training	Responsibilities, restrictions, confidentiality, spoofing, process for any data sharing, social media
Security, TRA	Regular audits, security & threat risk assessment annual-2 years




# Security Safeguards (2)

PRIVACY BREACH

LOCAL EMR	
Encryption	
Daily Back Up	2 levels of back up = local and cloud
Physical & Administrative Security	Audit logs
Training	Staff
Process	Designate, confidentiality agreements
ASP EMR	
Ask provider	Relying on provider- ask questions
Connectivity	Internet connectivity may be interrupted, redundant connection to the Internet from alternative supplier
Central Storage	
PHI local jurisdiction	





# *Information and Privacy Commissioner of Ontario (IPC)*

**PRIVACY BREACH**

---



EMR: EVERY STEP  
CONFERENCE

#OMDESC18

OntarioMD  
Empowered Practices. Enhanced Care.



# Important Recent Decisions by the IPC

---

**Decision 50:** A group medical clinic & a departing physician had a dispute over who was the HIC & whether an EMR service provider should have allowed the departing physician to extract his patients' health records. Matter went to court & resulted in a consent order granting physician ongoing access to his patients' records held by the clinic. Clinic complained to IPC that the EMR service provider improperly transferred patient files to departing physician.

**Conclusion:** IPC decided not to engage in a review as court had been involved & parties agreed to a consent motion. IPC commented on **importance of proactively establishing who is the HIC in multi-party relationships like group medical clinics.** IPC advised that agreements with EMR service providers should clarify who is the HIC & who can authorize record extractions.

## PRIVACY BREACH

---



# Important Recent Decisions by the IPC

---

**Decision 70:** Involved a Long-term care home where an employee took files home & lost records relating to 2 prospective residents. Home notified affected individuals. Home did not permit staff to take patient files home with them. Employee had done so due to workload issues and inexperience.

**Conclusion:** Home had not done enough to prevent breach. Home's policies & confidentiality agreement should have prohibited removal of files of PHI from facility. Make sure policies include a statement that identifiable PHI is not removed from the office unless you have approval or required by law.



# Important Recent Decisions by the IPC

**Decision 74:** A physician accessed medical records of a deceased individual (related by marriage & not providing care) using a hospital's EMR numerous times without authorization.



## PRIVACY BREACH



# Important Recent Decisions by the IPC

---

**Conclusion:** IPC determined **not** to issue any orders against the hospital or the physician.

Disciplinary consequences for physician were sufficient in the circumstances including: a **3 month suspension of hospital privileges** and on his return to practice, requirement to deliver present at Grand Rounds on topic of privacy.

Hospital **initially failed** to identify the unauthorized accesses, but once discovered took adequate steps including:

- (1) Installed a new auditing program to detect unauthorized access;
- (2) Updated Privacy and Confidentiality Policy;
- (3) Implemented a yearly electronic privacy training program for all staff, volunteers and learners and;
- (4) Strengthened the privacy warning on its electronic system to warn users that unauthorized use of PHI may result in disciplinary action.

---

## PRIVACY BREACH



# Check Up

## Scenario:

---

Police officers arrive at a family health organization (FHO) & ask the receptionist for a roster of patients who have active prescriptions for opioids. The police officers do not present a subpoena, search warrant, or other legal document permitting/ordering search & seizure.

*Is the FHO permitted to disclose a list of patients with active opioid prescriptions?*



# Check Up

---

*Is the family medical office permitted to disclose a list of patients with active opioid prescriptions?*

**NO** – In the absence of a court order, or other legal document permitting or obligating disclosure of PHI, the FHO is not permitted to disclose its patients' information to the police. The clinic's privacy obligations are unchanged – disclosure of patient information would breach these obligations.

**Note:** When PHI is disclosed to the police, physicians are encouraged to record the officer's name & badge number, the request for information, any information provided, & the authority for the disclosure. A photocopy of any search warrant or summons should be included in the patient's medical record. The police or Crown attorney will usually retain the originals, but will leave the physician with copies of the record, to ensure continuity of care.





# FUTURE



## loading...



# The Future...

- Online privacy & security training, facilitated by OntarioMD
- Privacy regime suggests increased government role as custodian of PHI
- Risk of confusion regarding custody & control of PHI & regarding who determines access rights
- Patient care is fundamental, easy of use, ease of access for purposes of treatment is critical



# Thank You!



The views expressed in this publication are the views of OntarioMD and do not necessarily reflect those of the Province.



EMR: EVERY STEP  
CONFERENCE

#OMDESC18

