Privacy & Security

+

Your EMR

Ariane Siegel

General Counsel & Chief Privacy Officer

OntarioMD

Empowered Practices. Enhanced Care.

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. Consent: The Building Block of Privacy
4. Ownership of Patient Records
5. The EMR Dashboard
6. Creating an accountable Medical Practice
7. OntarioMD's Privacy & Security Training
8. Reporting Privacy Breaches to IPC
9. Responding to Privacy Breaches
10. The Future

Why is Privacy Important to You?

The Role of OntarioMD

OntarioMD
Empowered Practices. Enhanced Care.

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

Our Delivery Partners

eHealth Ontario

Canada Health Infoway

Inforoute Santé du Canada

Ontario Local Health Integration Network

eConsult

otn.

Ontario Health Shared Services Ontario

OntarioMD Initiatives

- HEALTH REPORT MANAGER
- EMR PHYSICIAN DASHBOARD
- EMR PROGRESS ASSESSMENT TOOL
- EMR CERTIFICATION PROGRAM
- EMR PRACTICE ENHANCEMENT PROGRAM
- EMR: EVERY STEP CONFERENCE

Partnered Initiatives

- PROVINCIAL eCONSULT INITIATIVE
- eNOTIFICATIONS
- OLIS DEPLOYMENT
- ONE ID
- eREFERRAL
- PEER LEADER PROGRAM

The Privacy Landscape:
Basics

OntarioMD
Empowered Practices. Enhanced Care.

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**

Relevant Legislation & Regulations

PRIVACY

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

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**

Future Amendments to *PHIPA*

Upcoming on 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)**
- **Expanded obligations for HICs to report to IPC, based on seven expanded criterias & prescribed circumstances that are not mutually exclusive under section 12(3)**

Proposed:

- **Additional circumstances for notification to IPC, with possibility of annual reporting requirements**
- **Allow LHINs to carry out health care functions of CCACs & classify them as HICs**
- **Allow LHINs to rely on *assumed implied* consent to collect, use &/or disclose PHI for the provision of health care, unless otherwise aware that consent has been withheld or withdrawn**

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

Consent:
The Building Block of Privacy Law

OntarioMD
Empowered Practices. Enhanced Care.

Consent

- **May be (1) express, (2) implied, (3) or assumed implied, 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

Consent (1) – *EXPRESS*

Required when a HIC:

- discloses PHI to a non-HIC, another HIC for a purpose other than providing health care to individual;
- collects, uses or discloses PHI for marketing or market research; fundraising (if using more than name & address)

Consent (2) – *IMPLIED*

- **May be relied upon whenever a HIC uses PHI for most purposes under PHIPA**

  Examples:

  - Having a patient attending an appointment
  - Providing a referral to a specialist

Assumed Implied Consent

- **Allows a HIC to disclose PHI to another HIC within the patient's circle of care for healthcare purposes**

The Circle of Care

‘Circle of Care’

- The right for a HIC to assume a person’s consent when that same HIC is providing care to that same person

The ‘Lock Box’

- A person may withdraw consent – whether express or implied – through notice to the HIC (note: does not have retroactive effect)

How do you protect yourself & your practice?

Be proactive:

- Actively take the necessary steps to prevent the breach from occurring

Safeguard PHI:

- Use best practices to prevent loss, theft, or otherwise unauthorized access
- Train staff in all privacy & security measures

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

Ownership of Patient Health Records

OntarioMD
Empowered Practices. Enhanced Care.

Who Owns the Medical Record?

- **Content of medical records = patients**
- **Possession of medical records = physicians, or the person/organization responsible for file's creation (i.e., hospital or clinic)**

The Principle:

Patients have a right content of their record subject to some exceptions (e.g., likelihood of harm to the patient)

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**

OntarioMD

Right to Possession & Data Security

- 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)?**

The EMR Dashboard

OntarioMD
Empowered Practices. Enhanced Care.

What is the EMR Dashboard?

EMR Dashboard Proof of Concept

Scope (October 2016 – March 2018)

- **Physician 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)

OSCAREMR

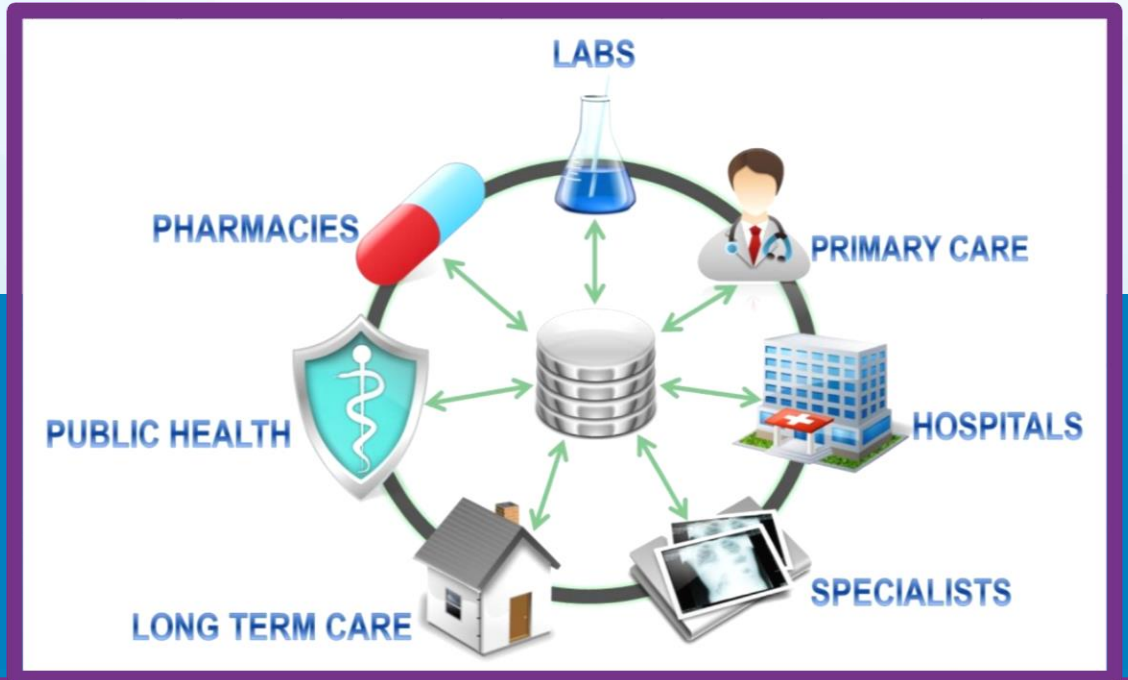
TELUS | HEALTH
Information for Life.

OntarioMD

Creating an accountable Medical Practice

OntarioMD
Empowered Practices. Enhanced Care.

Accountability



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
- **Limit** staff members' access to PHI &/or research data based on necessity

Introducing OntarioMD's Privacy & Security Training Tool

OntarioMD
Empowered Practices. Enhanced Care.

Privacy & Security Training

- OntarioMD has developed a *45 Minute* training tool for Ontario's community-based HICs necessary to connect to EHR Systems
- This application will:
  - *provide training about privacy & security*
  - *diminish portal user fatigue*

Strategy:

- Responds practically to needs of physicians & furthers OntarioMD's commitment to delivering quality health care, while maintaining interests of stakeholders

Privacy & Security Training

- CPSO, CMPA, OMA & other stakeholders – input on the content
- Physicians will receive **CME (continuing medical education)** credits upon completion of the program

Reporting a Privacy Breach to the Information and Privacy Commissioner (IPC)

OntarioMD
Empowered Practices. Enhanced Care.

Reporting a Privacy Breach

As of **October 1, 2017**, there are expanded obligations for HICs to report privacy breaches to the **IPC.** Under section 12(3), there are **SEVEN** categories that are **not** mutually exclusive; **more than one** can apply to a single privacy breach.

1. **Use or disclosure without authority**
2. **Stolen information**
3. **Further use or disclosure without authority after a breach**
4. **Pattern of similar breaches**
5. **Disciplinary action against a college member**
6. **Disciplinary action against a non-college member**
7. **Significant breach**

Responding to Privacy Breaches

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**

OntarioMD

Privacy Breaches: Further Concerns

- ***Snooping*: persons accessing PHI inappropriately**
  - **Note: recent disciplinary decisions by the Privacy Commissioner's Office have ordered fines in the tens of thousands of dollars to be paid by snooping clinical staff**
- **Patient files being lost or stolen**
- **Poorly encrypted storage – unencrypted laptops, cell phones, media devices, memory sticks, CDs**
  - **Consider: the 'internet of things'**
- **Email/fax sent to the wrong address**
- **Failure to log out or otherwise secure computer**
- **Discussing PHI with unauthorized individuals**

How to Respond to Privacy Concerns

****Risks can include legal, ethical, privacy, reputational – trust & best practices are critical in the world of electronic records****

- **Adopt only OntarioMD certified EMRs – *the certification process ensures that security safeguards are built-in***
- **Monitor against privacy breaches**
- **Avoid scenarios that invite risk of privacy breaches**
- **Reduce – institute or adjust controls**
- **Mitigate privacy liabilities**
- **Partner with another organization (i.e., a cybersecurity provider)**

Implement – Security Safeguards (1)

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 3rd 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)

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	

Privacy Training – Steps

- Meet regulatory compliance
- Prevent a privacy breach with privacy awareness
- Support risk management programs
- Keep your employees engaged to benefit:
  - Patient satisfaction
  - Business operations

- OntarioMD's Privacy & Security Training solution hopes to further the efficacy of privacy training beyond that of conventional methods & improve compliance with regulatory & professional standards.

Follow – The Privacy Breach Management Protocol

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

1. Identification
2. Reporting
3. Containment
4. Notification
5. Investigation
6. Remediation

The Privacy Breach Management Protocol (1)

1. **Identification**
   - Staff have an obligation to notify the health information **custodian as soon as they become aware** that PHI is (or may have been) stolen, lost, or accessed by unauthorized persons.
2. **Internal Reporting**
   - All staff should be aware of **when & to whom** the fact of a privacy breach should be reported.
   - Clarify the circumstances must be reported to others, including police, health regulatory colleges & the Information & Privacy Commissioner of Ontario.
3. **Containment**
   - HICs must immediately take reasonable steps to **contain the privacy breach** & to protect PHI from further threat, loss or unauthorized use or disclosure.

The Privacy Breach Management Protocol (2)

4. Notification

- PHIPA requires HICs to notify individuals at the first reasonable opportunity if their PHI is lost, stolen, or accessed by unauthorized persons
- As of October 1, 2017, PHIPA requires HICs to notify IPC about privacy breaches.

5. Investigation

- All privacy breaches must be conducted.

6. Remediation

- Keep a log of all privacy breaches.
- HICs should audit & monitor privacy breaches in order to identify patterns/trends in privacy breaches, & to ensure that appropriate safeguards are in place.

Thank You!