June 22, 2017

Privacy and Security

+

Your EMR

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 whose product(s) are being discussed in this program.

- **No Bias**

  There are no potential sources of bias.

OntarioMD
Empowered Practices. Enhanced Care.

Outline

1. The Role of OntarioMD
2. The Privacy Landscape: Basics
3. Consent: The Building Block of Privacy
4. The EMR Dashboard
5. Making Medical Practice Accountable
6. Governing Ownership of Patient Records
7. Handling Privacy Breaches
8. The Future

WHY IS PRIVACY IMPORTANT FOR YOU?

OntarioMD
Empowered Practices. Enhanced Care.

The Role of OntarioMD

OntarioMD
Empowered Practices. Enhanced Care.

OntarioMD & *PHIPA*

- OntarioMD is an **Agent** & **Health Information Network Provider** ("HINP").
  - 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 and security more accessible
  - By developing tools/software to make privacy and security more intuitive;
  - By reaching out to partners and stakeholders – the CMPA, IPC, eHealth Ontario – to develop collaborative, community-oriented privacy and security policies/tools

OntarioMD

Our Delivery Partners

eHealth Ontario
Otn
eConsult
Canada Health Infoway
Inforoute Santé du Canada
Ontario Local Health Integration Network
oaccac Ontario Association of Community Care Access Centres
acasco Association des Centres d'accès aux soins communautaires de l'Ontario

OntarioMD Initiatives

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

Partnered Initiatives

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

The Privacy Landscape:

Basics

OntarioMD
Empowered Practices. Enhanced Care.

Privacy: Complexities and the Law

- Doctor-patient relationship is governed by complex legislation and confidentiality requirements

- The demands to preserve privacy and 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

OntarioMD
Empowered Practices. Enhanced Care.

The Personal Health Information Protection Act

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

- **"Health Information Custodians"** (HIC) under *PHIPA* = physicians and healthcare providers

Key Principles:

- Physician-patient relationship is built on trust
- 'Consent-based' legislation

Important Updates to *PHIPA* (1)

1. **Notification:**
   - HICs are required to notify any individuals affected by improper disclosure of PHI

2. **Extended Reporting Obligations:**
   i. Obligations for HICs extended to include: (1) regulated health professionals under the RHPA, (2) members of the College of Social Workers, (3) and Social Services Workers
   ii. **HICs are required to make a report to the relevant regulatory college within 30 days of a privacy breach**

Important Updates to *PHIPA* (2)

4. **Judicial Prosecution:**
   - Courts have explicit authority to take precautionary measures to protect PHI from disclosure in judicial proceedings
5. **Doubled Fines for Privacy Offenses**
6. **Consent Override:**
   - In extreme circumstances: the option to override consent regulation where a significant risk of bodily harm is anticipated and may be prevented through disclosure

Future Amendments to *PHIPA*

Upcoming:

- Requirement to give notice to the **Information and Privacy Commissioner (IPC)** for any theft, loss or unauthorized use or disclosure of PHI **(July 1, 2017)**

Proposed:

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

Critical Concerns for Health Care

- Privacy law is a rapidly developing and 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 and the health care profession

Summary – Your Privacy Obligations

- To notify person(s) affected if their PHI is used or disclosed without proper authority
- Discretionary Consent Overrides
  - Circumstances where it may be necessary to override consent directives to otherwise eliminate or reduce significant risk of serious bodily harm
- Report to regulatory colleges
- How you use the PHI:
  - Express or assumed implied consent
  - Responsibility for agents

Consent

The Building Block of Privacy

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; and
  - (iv) not be obtained through deception or coercion

OntarioMD
Empowered Practices. Enhanced Care.

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

OntarioMD
Empowered Practices. Enhanced Care.

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)

Check Up

Judy visits her family physician, Dr. Larsen, complaining of major headaches. Dr. Larsen examines Judy and asks her a series of questions about her medication, personal and family medical history. He also conducts a physical examination.

Dr. Larsen refers Judy to a cardiologist. He writes a referral letter detailing Judy's symptoms, relevant medical history and the results of his examination.

Is Dr. Larsen permitted to disclose this information? Is he required to collect Judy's consent? Is the cardiologist permitted to collect this information?

A. No, Dr. Larsen and the cardiologist are not allowed to disclose or collect this information without her express consent.

B. Yes, both Dr. Larsen and the cardiologist can rely on Judy's implied consent to disclose and collect information.

Check Up – Answer

B. The information is being disclosed to another physician for the purpose of providing health care to Judy. She had not 'locked' any information collected. Dr. Larsen and the cardiologist can rely on Judy's implied consent to disclose and collect information. They are both within Judy's circle of care.

How to 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 and security measures

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

The
EMR Dashboard

OntarioMD
Empowered Practices. Enhanced Care.

What is the EMR Dashboard?

OntarioMD
Empowered Practices. Enhanced Care.

EMR Physician Dashboard Proof of Concept

Scope (October 2016 – March 2017)

- **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 and EMRs:
    - OSCAR EMR (OSCAR 15)
    - TELUS Health (PS Suite, Med Access)

OSCAREMR

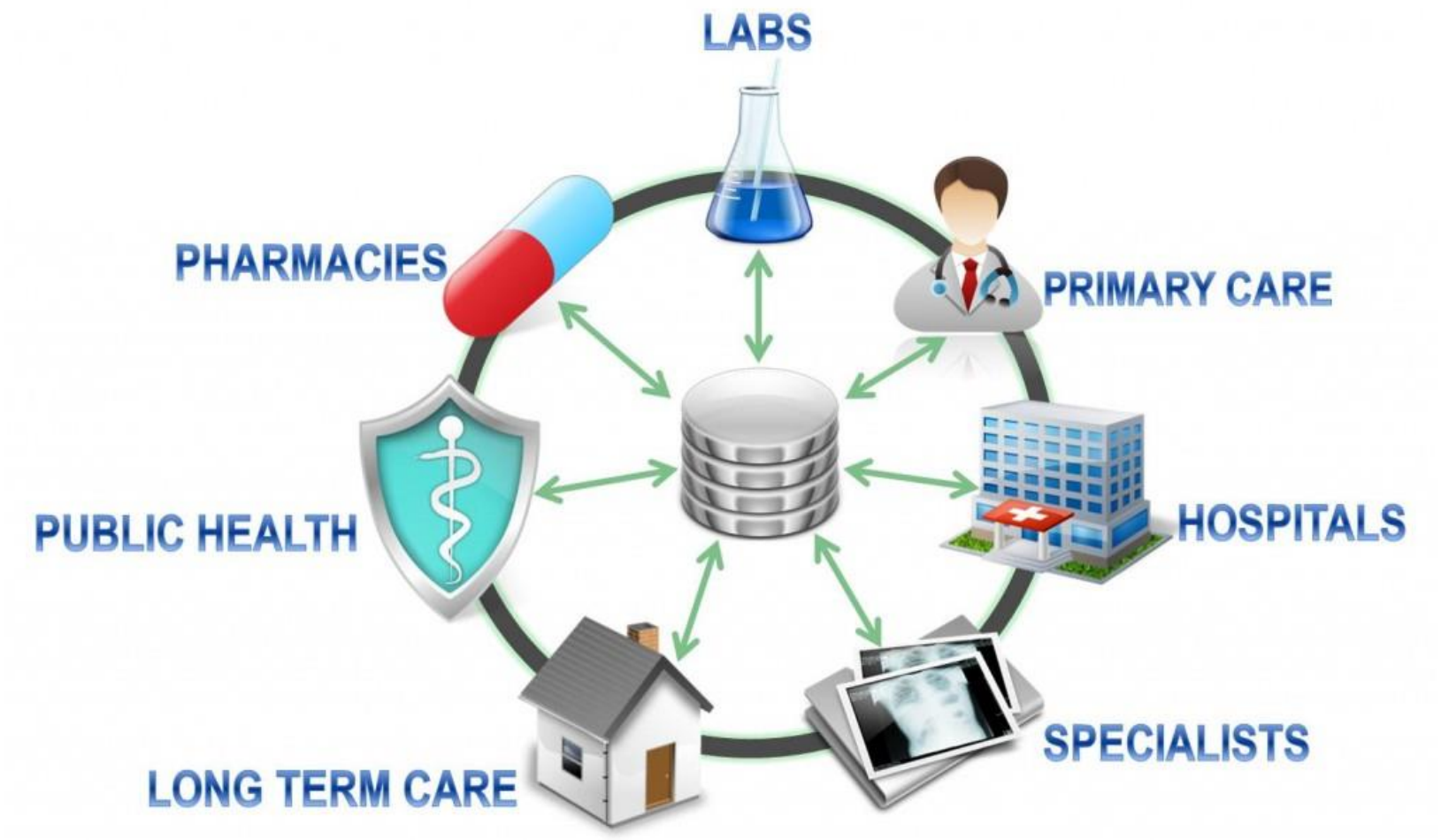
TELUS | HEALTH
Information for Life.

OntarioMD
Empowered Practices. Enhanced Care.

Making Medical Practice Accountable

OntarioMD
Empowered Practices. Enhanced Care.

Accountability



OntarioMD
Empowered Practices. Enhanced Care.

Best Practices: Act Accountable (1)

- Identify responsibilities and 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, and ethical standards

Best Practices: Act Accountable (1)

- 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 team members' access to PHI and/or research data based on necessity

Governing
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)

- Transferring custody and control of patient records is governed transfer and retention regulations

OntarioMD
Empowered Practices. Enhanced Care.

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; and
  - 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 and transferring patient records;
  - Govern custody and control;
  - Limit access to the content of medical records;
  - Control transfer and 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)?

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 and PI which are extremely valuable on the black market**

OntarioMD
Empowered Practices. Enhanced Care.

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 and 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)

OntarioMD
Empowered Practices. Enhanced Care.

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
Admin/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 • **Use complex passwords and store these securely (NOT on post-its)**

Security Safeguards (2)

LOCAL EMR	
Encryption	
Daily Back Up	• 2 levels of back up = local and cloud
Physical and 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 – Requirements

- Meet regulatory compliance
- Prevent a privacy breach with privacy awareness
- Support risk management programs
- Keep your employees engaged to benefit:
  - Patient satisfaction
  - Business operations
- More effective than conventional training and in compliance with regulation and 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 and to whom** the fact of a privacy breach should be reported.
   - Clarify the circumstances must be reported to others, including police, health regulatory colleges and the Information and Privacy Commissioner of Ontario.
3. **Containment**
   - HICs must immediately take reasonable steps to **contain the privacy breach** and 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.
5. **Investigation**
   - All privacy breaches **must be conducted**.
6. **Remediation**
   - Keep a log of all privacy breaches.
   - HICs should **audit and monitor** privacy breaches in order to identify patterns/trends in privacy breaches, and to ensure that appropriate safeguards are in place.

Further Considerations – Breach Protocol

- **ASK FOR HELP!**
  - Tools to help manage the breach responsibly, professionally, and mitigate the harm done by the breach.
  - Make preventative plan and breach response plan
  - Consider cyber breach liability insurance
  - Build privacy into every step and service that you provide to patients

DO'S

DONT'S

- ✓ **DO prepare and create a culture of privacy**
- ✓ DO understand accountability
- ✓ DO complete requisite form
- ✓ DO follow best practices
- ✓ DO follow good ethical standards
- ✓ DO identify obligations- depends on circumstances.
- ✓ DO share responsibility for protecting unauthorized access to or disclosure of PHI
- ✓ DO cooperate
- ✓ DO view PHI for individuals who you are providing healthcare

- ✗ DON'T put PHI on any devices
- ✗ DON'T email, text, print or fax PHI from personal accounts
- ✗ DON'T forward emails without checking for PHI
- ✗ DON'T expect others to be diligent
- ✗ DON'T delete immediately, report first
- ✗ DON'T share confidential information
- ✗ DON'T provide unnecessary confidential information to co-workers
- ✗ DON'T aggregate contact information on your own directories or devices.
- ✗ DON'T re-forward or resend incident
- ✗ **DON'T share Personal, Confidential or Personal Health Information**

OntarioMD
Empowered Practices. Enhanced Care.

The Future

OntarioMD
Empowered Practices. Enhanced Care.

The Future…

- Waiting for details on consent and breach
- Privacy regime suggests increased government role as custodian of PHI
- Risk of confusion regarding custody and control of PHI
- Risk of confusion regarding who determines access rights
- Patient care is fundamental, easy of use, ease of access for purposes of treatment is critical

Thank you!