SEPTEMBER 22, 2016

MOVING BEYOND THE EMR: PRIVACY & MEDICAL PRACTICE

ARIANE SIEGEL
General Counsel & Chief Privacy Officer, OntarioMD

OntarioMD
Empowered Practices. Enhanced Care.

FACULTY / PRESENTER DISCLOSURE

- **Presenter:** Ariane Siegel

- **Relationships with commercial interests:**
  - No relationship with commercial interests

DISCLOSURE OF COMMERCIAL SUPPORT

- This program has not received financial support or in-kind support from any organization
- **Potential for conflict(s) 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.

MITIGATING POTENTIAL BIAS

- There are no potential sources of bias.

WHY IS PRIVACY IMPORTANT FOR YOU?

OUTLINE

1. PRIVACY LANDSCAPE BASICS
2. PHIPA: CHANGES & IMPLICATIONS
3. PRIVACY BREACH MANAGEMENT
4. OWNERSHIP OF DATA
5. SECURITY AND RANSOMWARE

PRIVACY LANDSCAPE BASICS

OntarioMD
Empowered Practices. Enhanced Care.

PRIVACY LAW AND OTHER LEGAL OBLIGATIONS

PRIVACY

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

OTHER

- MEDICINE ACT
- CPSO GUIDELINES
- COURT ORDERS

PHIPA

- Bill 119 -Royal Assent received on May 18, 2016
- AMENDMENTS TO PHIPA to make certain related amendments and to repeal and replace the Quality of Care Information Privacy Act, 2004.
- New standard of protecting privacy & confidentiality of Personal Health Information (PHI)

PHIPA: CHANGES & IMPLICATIONS

OntarioMD
Empowered Practices. Enhanced Care.

KEY REFORMS TO PHIPA INCLUDE:

- **Doubling** the maximum fines for privacy offences
  - Individuals: $50,000 to $100,000
  - Organizations: $250,000 to $500,000
  - Strengthen process to prosecute offences removes requirement that prosecutions be commenced with 6 months of when alleged offence occurred.

KEY REFORMS TO PHIPA INCLUDE:

- **Expanded Definition of "Use"**
  - "to **view**, handle or otherwise deal with the information".
  - intended to hold those who snoop into health records liable.
- **Electronic Health Records (EHR) –**
  - **Definition**: computerized medical record shared between health care providers that provide patient EHRs may include a whole range of data

KEY REFORMS TO PHIPA INCLUDE:

- **Electronic Health Records (EHR) –**
  - S. 55 “prescribed organization has the power and the duty to develop and maintain the electronic health record.”
  - PO will manage and integrate personal health information and oversee the EHR, including monitoring and logging access.
  - Concept: Must contribute to EHR

KEY REFORMS TO PHIPA INCLUDE:

- **Notification Duties -** Health Information Custodians (HICs) must notify affected individuals if Personal Health Information (PHI) about an individual in its custody or control is used or disclosed without authority.
- **Consent Overrides –** Circumstances where a consent directive could be overridden, specifically, on consent, or where disclosure is necessary to eliminate or reduce the significant risk of serious bodily harm

KEY REFORMS TO PHIPA INCLUDE:

Increased Role of :

- Ontario Government (access without consent, custodian)

- IPC - File complaints

KEY REFORMS TO PHIPA INCLUDE:

- **Consent Directives** – HIPA "lock-box" provisions EHR context.
- Individuals can withdraw consent to the collection, use and disclosure of their PHI. HICs would be notified of the directive but would not be provided any of the PHI.
- Medicine Act – follow up

HOW TO PROTECT YOURSELF AND 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.

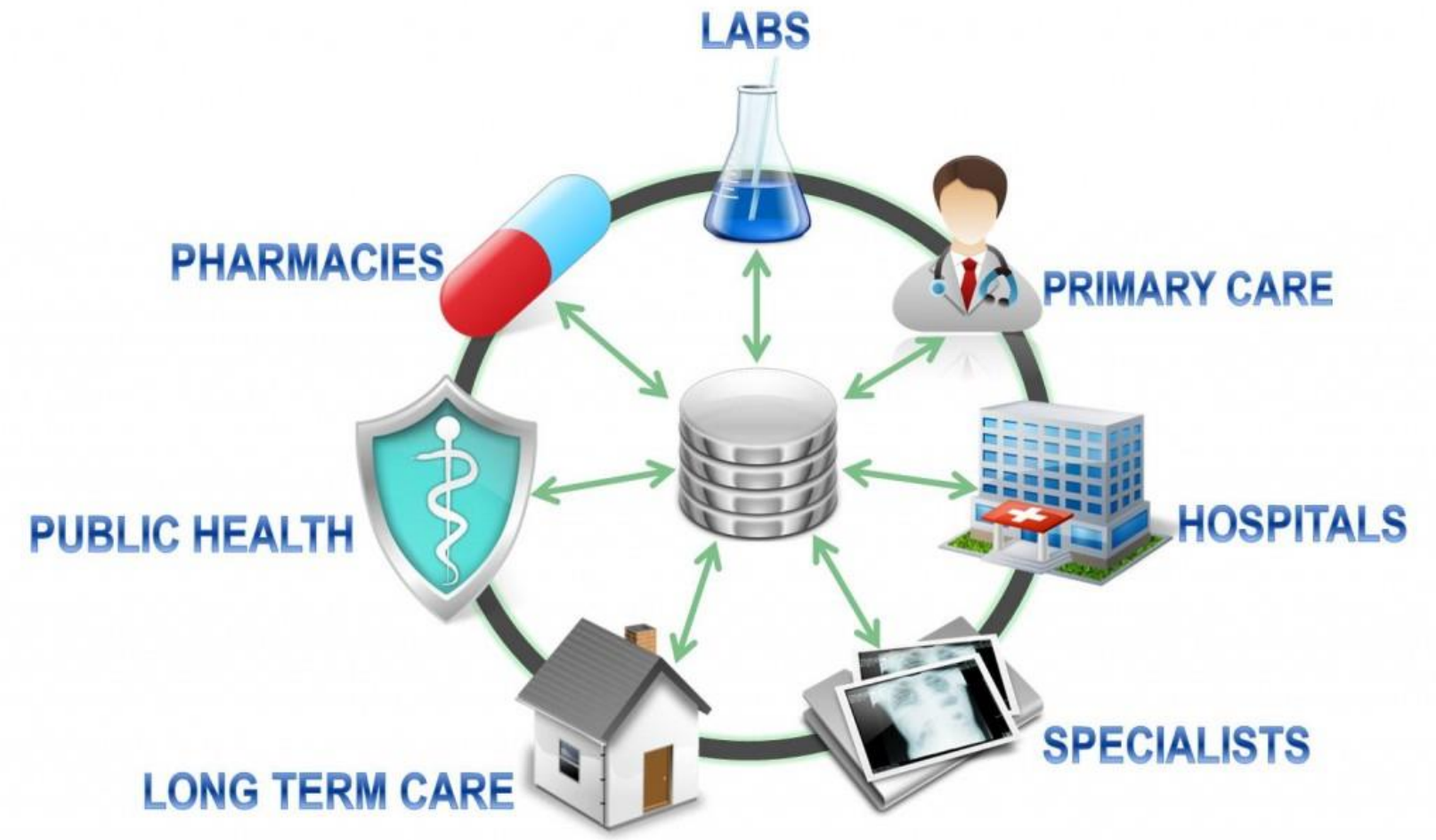
- **Privacy has to support medical practice**

IMPLICATIONS OF PHIPA

Expanded Responsibilities

- HICs responsible for agents
- Accountability
- Informed consent, safeguards, training, retention, training
- S. 17.1 Reporting to governing College (Regulated Health Professions Act) and member of College of Social Workers and Social Service Workers

ACCOUNTABILITY



OntarioMD
Empowered Practices. Enhanced Care.

HANDLING PRIVACY BREACHES

OntarioMD
Empowered Practices. Enhanced Care.

EXAMPLES OF PRIVACY BREACHES

- Talking in public areas, posting on Internet, sharing with the wrong person
- Lost/stolen or improperly disposed paper documents, films, notebooks, medication bottles
- Lost/stolen unencrypted laptops, tablets, cellphones, media devices (video and audio recordings)
- Lost/stolen unencrypted, CDs, flash drives, memory sticks
- Hacking of unprotected computer systems
- Email or faxes sent to the wrong address, wrong person, or wrong number
- Users not logging out of computer systems, allowing others to access their computer or system

DATA BREACHES

- **UNINTENTIONAL**
  - A hospital or physician accidentally sends a screenshot containing personal health information.
- **MALICIOUS**
  - Intending or intended to do harm
  - CMA case study

OntarioMD
Empowered Practices. Enhanced Care.

SEVERITY LEVELS

HIGH: Privacy breach involving multiple patients

MEDIUM: Privacy breach involving a single patient

LOW: Potential privacy breach

OntarioMD
Empowered Practices. Enhanced Care.

CHECK UP

You are very upset because a young patient has just coded and was not resuscitated. You want to share this experience and your thoughts and feelings with your family and friends on Facebook. What must you consider before doing this?

- A. Posting this on Facebook is OK as long as you do not identify the patient by name, or identify the hospital, and you are limiting the recipients to your friends and family.
- B. You cannot post anything on Facebook that could possibly lead to identification of the patient.

CHECK UP

B. Don't post anything on Facebook that could lead to identification of the patient.

- Facebook is considered public domain.
- Posting clinical details without prior authorization is a violation of a patient's privacy.
- Your Facebook Profile may identify your occupation and your place of work. When linked with your posting, and with any other publicly available information, the additional details may identify the patient in inquiry.
- Information you obtain from patient/provider relationship is confidential.

DO'S

DON'TS

- ✓ **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

- ✗ 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.

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

PRIVACY BREACH MANAGEMENT PROTOCOL

- **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.
- **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.
- **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.

PRIVACY BREACH MANAGEMENT PROTOCOL

- **Notification**
  - PHIPA requires HICs to notify individuals at the **first reasonable opportunity** if their PHI is lost, stolen, or accessed by unauthorized persons.
- **Investigation**
  - All privacy breaches **must be conducted**.
- **Remediation**
  - Keep a log of all privacy breaches.
  - HICs should **audit and monitor** the log of privacy breaches in order to identify patterns or trends in privacy breaches, and to ensure that appropriate administrative, physical or technical safeguards.

PRIVACY BREACH MANAGEMENT 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

OntarioMD
Empowered Practices. Enhanced Care.

CHECK UP

Your printer breaks down in the middle of printing a patient's requisition form. You hire a technician to come in to fix the machine. They fix the printer and out spews the patient's records that the technician may see. What happens?

- A. It is okay as has a contract regarding confidentiality. Just remind technician of duties of confidentiality.
- B. This is a breach of data and the patient needs to be notified.

CHECK UP

A. The practice has a service and confidentiality agreement in place with the vendor. The technician is under a duty not to use any PHI that may be viewed incidentally to the provision of a necessary service.

CHECK UP

You're a physician. Your boyfriend notified you that his sister was recently admitted to hospital and is in critical condition. You both have a great relationship, and you would like to know how she's doing and see if you can help. May you access her records to check on her condition?

- A. It is okay as she's my boyfriend's sister, so you are sure she wouldn't mind you looking at her records
- B. You already have approval to access patient clinical systems, so no one will know that you accessed it
- C. It is not necessary for your job, so you would be violating the patient's privacy by accessing her records. You should contact her family to check on her condition.

OntarioMD
Empowered Practices. Enhanced Care.

CHECK UP

- **C. It is not necessary for your job, so you would be violating the patient's privacy by accessing her records. You should contact her family to check on her condition.**

OWNERSHIP OF DATA

OntarioMD
Empowered Practices. Enhanced Care.

WHO OWNS THE MEDICAL RECORD?

- **Content** of a medical record: patient
- **Record of a medical record**: physician, person or organization responsible of its creation. i.e. hospital or clinic.
- **What this means:** Patients have a right content of their record subject to certain exceptions (e.g. likelihood of harm to the patient).

OntarioMD
Empowered Practices. Enhanced Care.

RELOCATION

- Responsible for records retention requirements, whether or not you will be providing ongoing health care to patients.

- If want to transfer custody of records, ensure that arrangements you make for record transfer and retention comply with law.

MEDICAL RECORDS IN A GROUP PRACTICE OR EMPLOYMENT SETTING?

- Contract
  - Responsibility for maintaining and transferring patient records.
  - Ongoing custody and control
  - Reasonable access to the content of the medical records
- Dissolution of group practice: Who gets the record?
- Physician employees agreement re: patient record retention, access and transfer.

CHECK UP

Judy goes to her family physician Dr. Larsen complaining of major headaches. Dr. Larsen examines Judy and asks her a series of questions relating to her medication, health history and health history of her family. He also conducts an examination.

Dr. Larsen indicates to Judy that he is going to refer her to a cardiologist, Dr. Cooper. He writes a referral letter detailing Judy's symptoms, her health history and the results of his examination.

Is Dr. Larsen permitted to disclose this information? Does he require Judy to sign a consent form? Is Dr. Cooper permitted to collect this information?

- A. No, Dr. Larsen and Dr. Cooper were not allowed to disclose or collect this information without her express consent.
- B. Yes, Dr. Larsen and Dr. Cooper can rely on Judy's implied consent to disclose and collect the information.

CHECK UP

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

SECURITY AND RANSOMWARE

OntarioMD
Empowered Practices. Enhanced Care.

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

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	

OntarioMD
Empowered Practices. Enhanced Care.

SECURITY – WHAT IS REASONABLE?

Lessons from a dating site for married people:

- Inadequate authentication processes for remote access
- Encryption on web communications but encryption keys were stored as plain, clearly identifiable text.
- Poor key and password management practices. ‘Shared secret’ for remote access server on Google drive.
- Storage of passwords as plain, clearly identifiable text in emails and text files.

RANSOMWARE

- Health care professionals and organizations are being targeted by cybercriminals on a regular and increasing basis.
- EMRs provide a treasure trove of both PHI and PI which are extremely valuable on the black market.
- **Ransomware** is the practice of holding hostage a computer system or the data it contains, and then extorting money from its rightful owner.

RANSOMWARE

- For more information & for specific steps to address the threat of a ransomware: Please refer to the **Bulletin** available at our booth today or contact your OntarioMD Practice Management Consultant.

CHECK UP

You got an email with a link to a free cruise you have just won to the Bahamas. You click on the link and suddenly your screen goes haywire and you get a message telling you your data has just been taken and to get it back you will need to pay $18,000. You check and you cannot access patient files on your EMR. Help!

- A. Call your Practice Management Consultant at OntarioMD
- B. Call your EMR provider
- C. Go home and take some Tylenol

CHECK UP

Answer is A and B.

- A. Call your Practice Management Consultant at OntarioMD
- B. Call your EMR provider

Luckily, after consultation you realize that you have two levels of back up. No data was accessed by a third party. Your technology support company is able to restore your data Happy day!

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!

Questions?

www.ontariomd.ca

OntarioMD
Empowered Practices. Enhanced Care.