PRIVACY & SECURITY + YOUR EMR

PRIVACY
TRAINING AND RESOURCES

Ariane Siegel
General Counsel & Chief Privacy Officer
June 13, 2019

OntarioMD

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. RELATIONSHIPS WITIN THE HEALTHCARE SYSTEM
3. MANAGING THE COMPLEXITIES OF THE HEALTHCARE SYSTEM AND THE LAW
4. CLINICIAN OBLIGATIONS
5. DATA GOVERNANCE
   A. How to handle PHI
6. ACCESS v. OWNERSHIP
7. ACCOUNTABILITY: HOW TO CREATE AN ACCOUNTABLE PRACTICE
8. PROTECT YOUR PRACTICE
   A. Safeguards
   B. Privacy Breach Management Protocol
   C. Privacy & Security Training

THE ROLE OF ONTARIOMD

Health Information Network Provider.

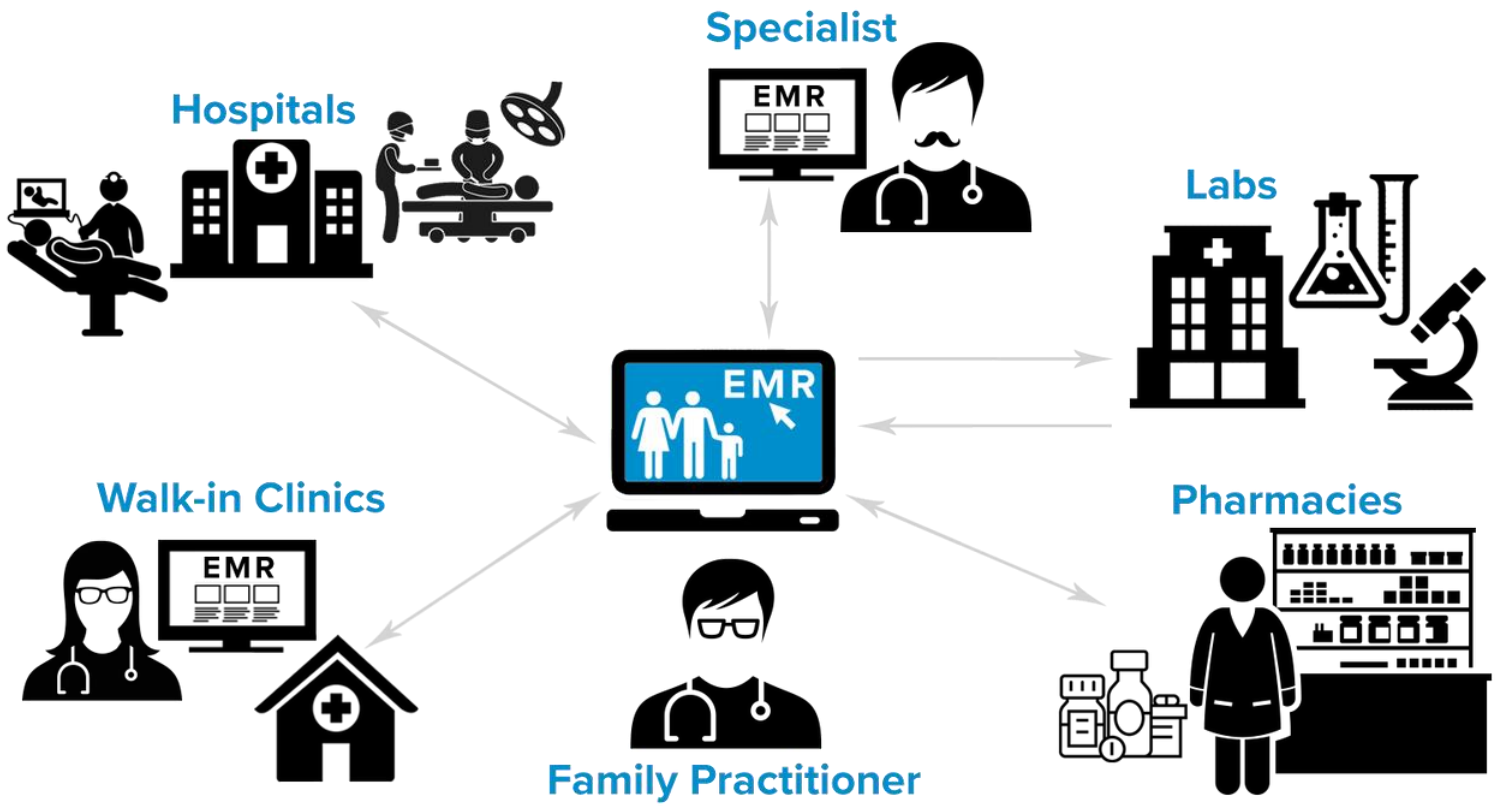
Serves as an **Agent** to Health Information Custodians (HICS).

Mission: Make Privacy & Security Training more accessible and help clinicians better understand their obligations.

CIRCLE OF CARE

Depending on Patient Tim's health, Dr. Chris may refer Patient Tim to other health care professionals. These professionals will form part of Patient Tim's Circle of Care.

How do OHTS fit in?



PRIVACY: COMPLEXITIES & THE LAW

Dr. Chris' and Patient Tim's relationship is governed by complex legislation & confidentiality requirements.

The demands to preserve privacy & confidentiality are complicated by the pressure to ensure:

- Better health information sharing
- Increased efficiency of health care

PERSONAL HEALTH INFORMATION PROTECTION ACT

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

- Under *PHIPA,* physicians & healthcare providers are health information custodians (HICs)

Key Principles:

Physician-patient relationship is built on trust

- **"Consent-based"** legislation

THE DOCTOR WILL SEE YOU NOW…

In addition to providing patient care, Dr. Chris, as a HIC, has many obligations to fulfill.

DATA GOVERNANCE

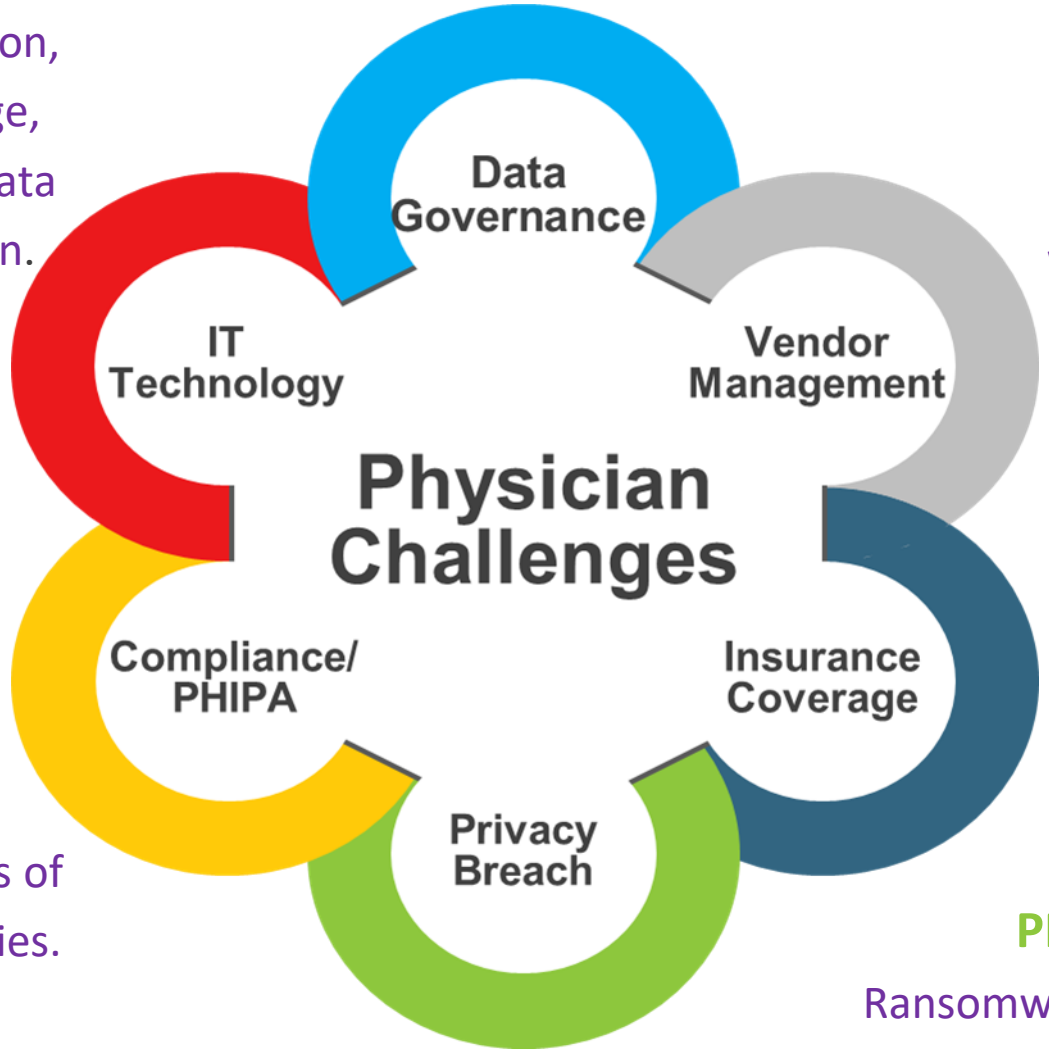
Issues related to data deletion, data ownership, data storage, data use, data portability, data retention and data migration.

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.



VENDOR MANAGEMENT

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

INSURANCE COVERAGE

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

PRIVACY BREACH

Ransomware and Response Plan.

DATA GOVERNANCE

Federal and Provincial Laws

Privacy Commissioner's Requirements and Findings

Professional Obligations as per the CPSO

CONSENT

What forms of consent does Dr. Chris need to obtain from Patient Tim in order to collect and use his PHI?

Express
Implied
Assumed Implied

USE- VIEWER

What would a reasonable physician do?

In the context of that particular provision of care

Review relevant prescribing data (i.e., NMS/HQO).

Evolving expectations eg- review information in digital tools- **Digital Health Drug Repository** when available/accessible.

DISCLOSURE

Once Patient Tim's PHI is in DR. Chris' EMR, can Dr. Chris share this the data with other parties?

IMPORTANT RECENT IPC DECISIONS

EQUIFAX FEDERAL OPC

- Disclosing party of PI remains accountable, even after 3rd party collects and uses data.
- Disclosure of data across borders requires consent.
    - Form of consent depends on sensitivity of information and risk of harm.

Decision 80 – DISCLOSING INFORMATION TO THE MEDIA

- Hospital responded to media request about a deceased patient. The patient had been the subject of an HPARB decision. While the name of the patient was not disclosed during communications with the media, IPC found the disclosure was inappropriate as the patient's PHI was disclosed without consent.
- **Rule**: To determine if the information being disseminated includes PHI, one must consider whether it is reasonably foreseeable, in the circumstances, that others without that special knowledge of the situation, could identify the patient by combining the information provided by the [individual] with other available information.

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

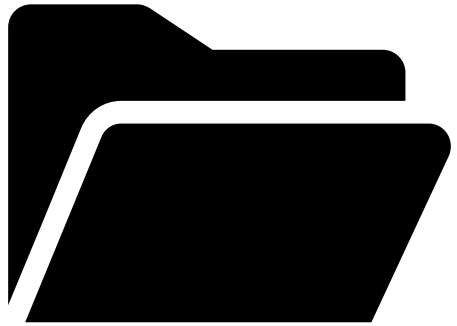
- Healthcare databases not compellable
- Phillips Morris cannot see de-identified raw data (s.2(5)(B) of the Tobacco Damages and Health Care Costs Recovery Act)

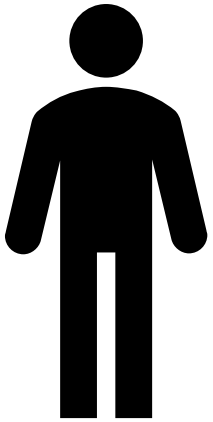
RETENTION, RELOCATION & DESTRUCTION

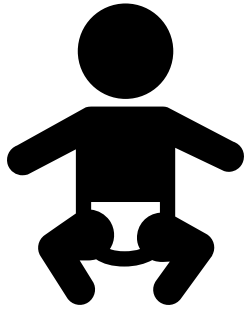
Physicians are responsible for retaining patient records, regardless of whether they are continuing to provide care to the respective patient(s):

- Adults: 10 years from date of last entry in record
- Children: 10 years from day patient reached or would have reached 18

Transferring custody & control of patient records is governed by transfer & retention regulations.







WHO OWNS THE MEDICAL RECORD?

Physical or Digital Medical Record(s)

- Clinician or Entity that created the Medical Record (i.e. hospital or clinic)

Shared Custody and Control

The Principle: Patients have a right to reasonable access to examine and copy their records.

⚠ **Some Exceptions**

- likelihood of harm to patient (**IPC Decision 52**)

RIGHTS TO POSSESSION

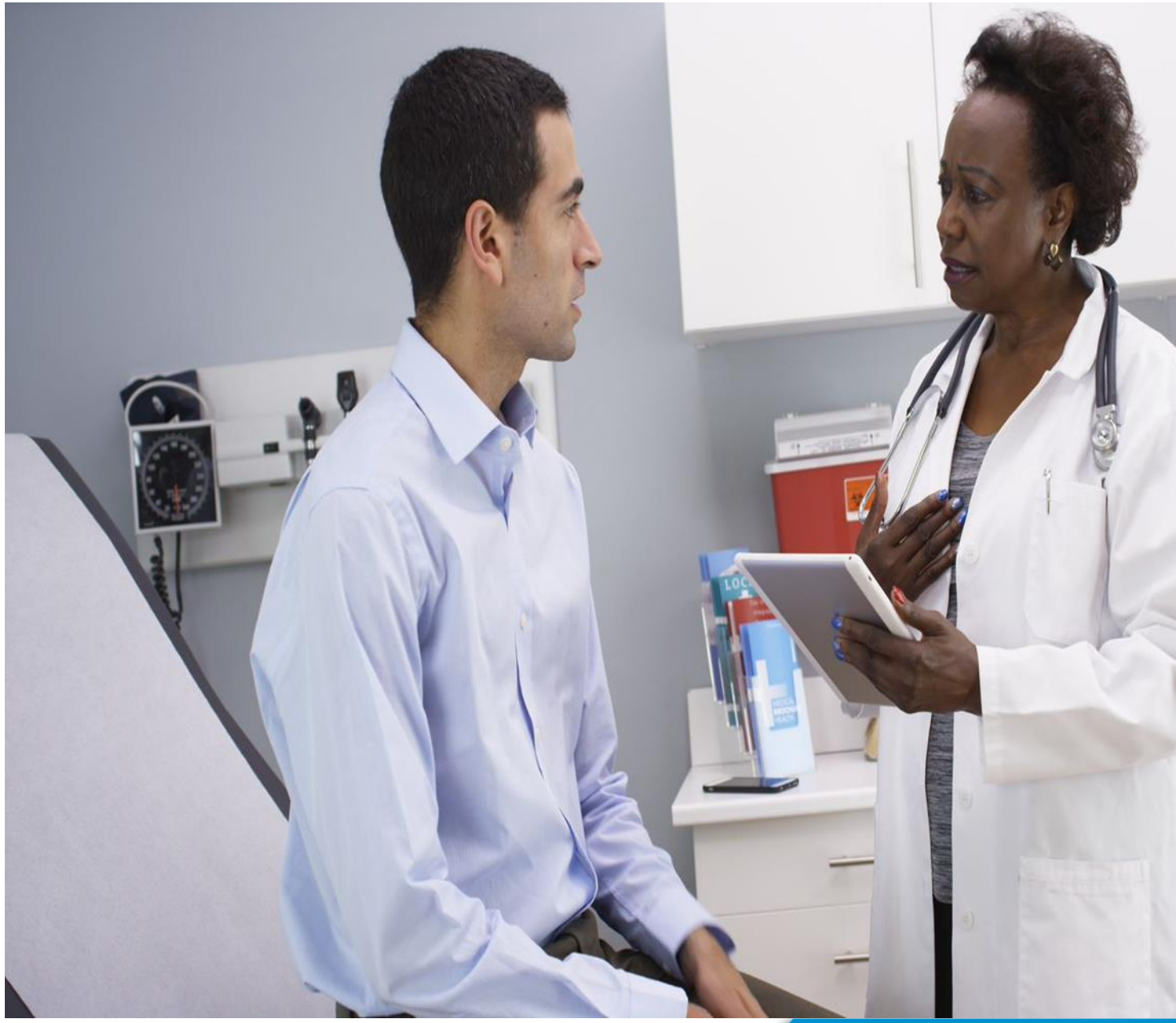
Fiduciary Duty

- an obligation to place patients' interests ahead of physicians

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

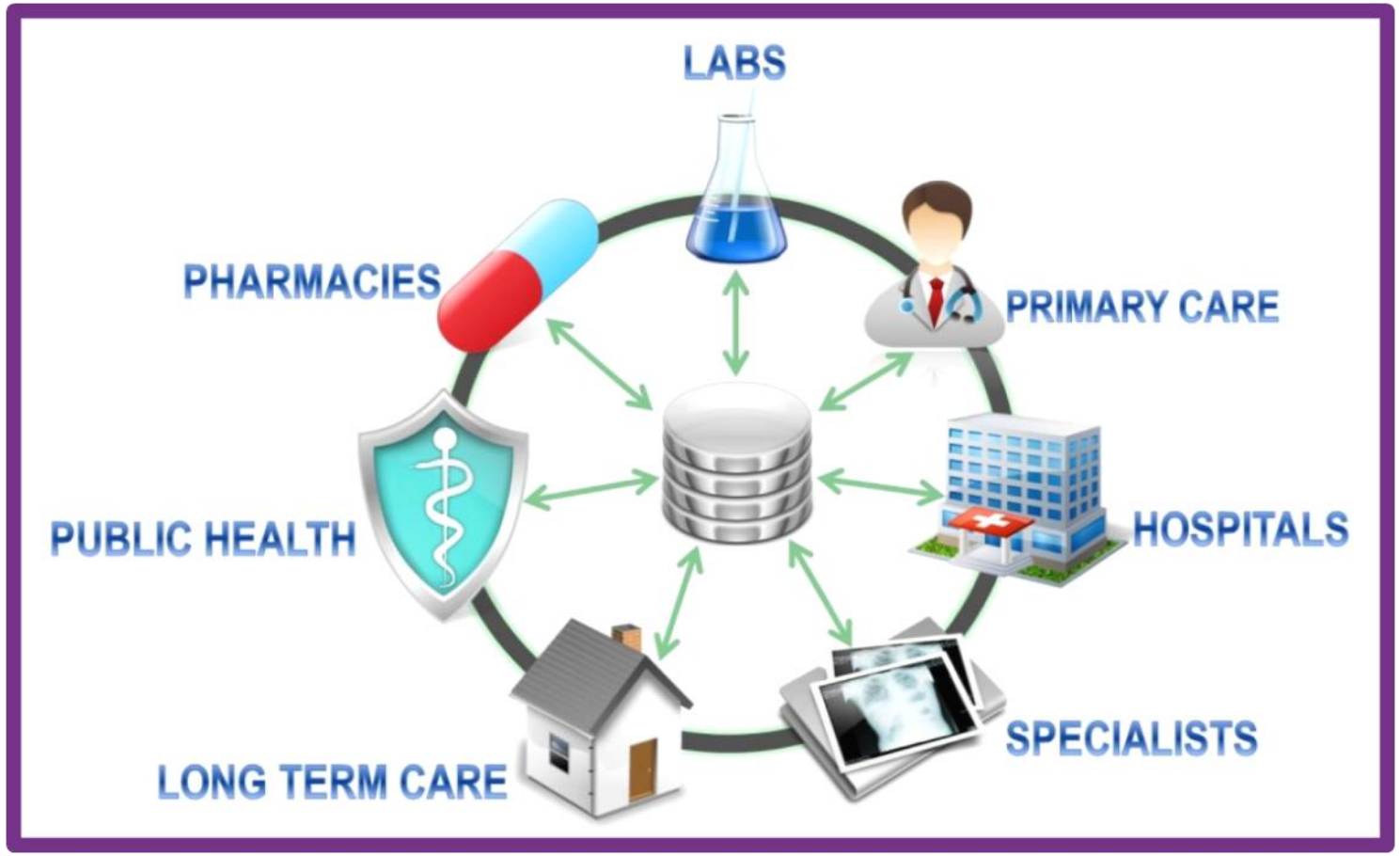
Contractual obligations may:

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

Legal Question:

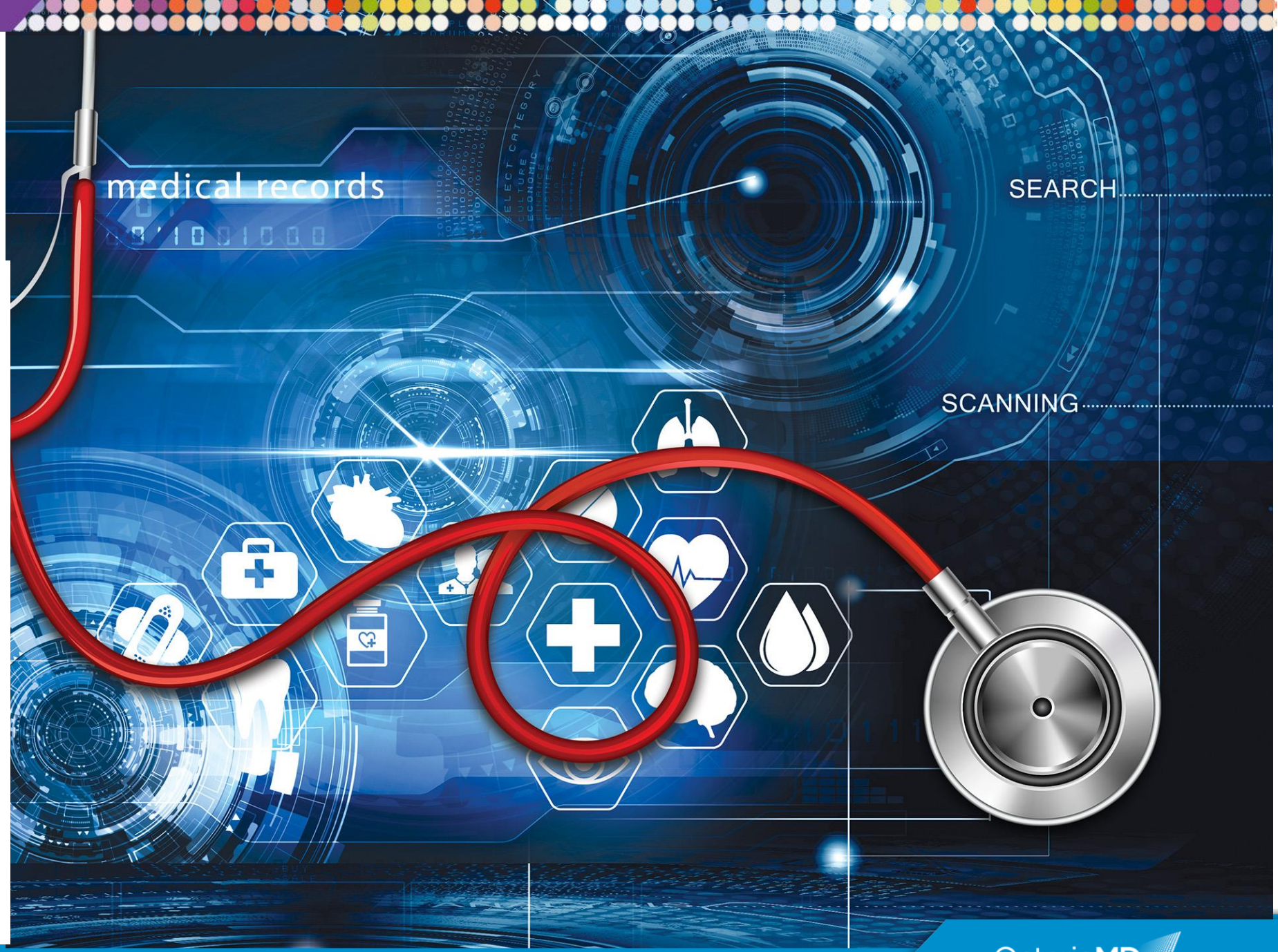
Who has the ultimate right to possession over shared, EMR-hosted records? The physician, or the clinic (the EMR host – through contract)?

CREATING AN ACCOUNTABLE PRACTICE



BEST PRACTICES: TO BE ACCOUNTABLE

PROTECT YOUR PRACTICE



SAFEGUARDS

Update Technology

- Windows 7

Encryption

Password

UP-TO-DATE IMPLEMENTATION

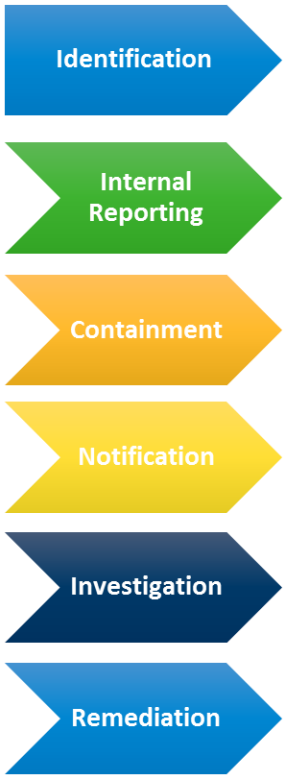
PHYSICAL SAFEGUARDS	
Firewall, encryption	Credential-based access (2 factor authentication), password protection, masking, encryption, time outs
Daily Back Up	Local and cloud
Out of public view	Away from public view, don't store devices in car, encrypted USB keys, establish secure areas, sign in and badges, server in secure area, log out
Audit Logs	Authentication, warning flags for consent directives
Anti-virus	Operating System/Software - automatic updates, active firewall on networks (WINDOWS 7- 2020 ISSUE)
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

IMPLEMENTATION

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	

THE PRIVACY BREACH MANAGEMENT PROTOCOOL

SIX Steps HICs Must Address



- Response Plan
- Cyberliability Insurance

OntarioMD

PRIVACY & SECURITY TRAINING MODULE

ANYTIME, ANY PLACE, ANY DEVICE

Launch Privacy and Security Training Now

THE COLLEGE OF PHYSICIANS AND SURGEONS OF ONTARIO

eHealth Ontario

OMA ONTARIO MEDICAL ASSOCIATION

CMPA.

Information and Privacy Commissioner Ontario, Canada

OntarioMD

THE BENEFITS

Complimentary
Comprehensive
Current
Accredited
Accessible
Mobile
Certificate of Completion

PRIVACY AND SECURITY ENHANCES AND ENABLES PATIENT CARE

Questions and Discussion? Follow us on social media!

- www.ontariomd.ca
- twitter.com/ontarioemrs
- www.linkedin.com/company/ontariomd
- ontariomd.blog
- facebook.com/ontariomd
- vimeo.com/ontariomd

OntarioMD

supporting clinicians' digital health needs

Thank You!

Ariane. Siegel@OntarioMD.com