W5 H

PRIVACY & SECURITY + DIGITAL HEALTH TOOLS

Ariane Siegel
General Counsel & Chief Privacy Officer

September 26, 2019

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 is an employee of OntarioMD she has not received payment or funding from any other 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 – apart from the perspective of the primary care provider in the community

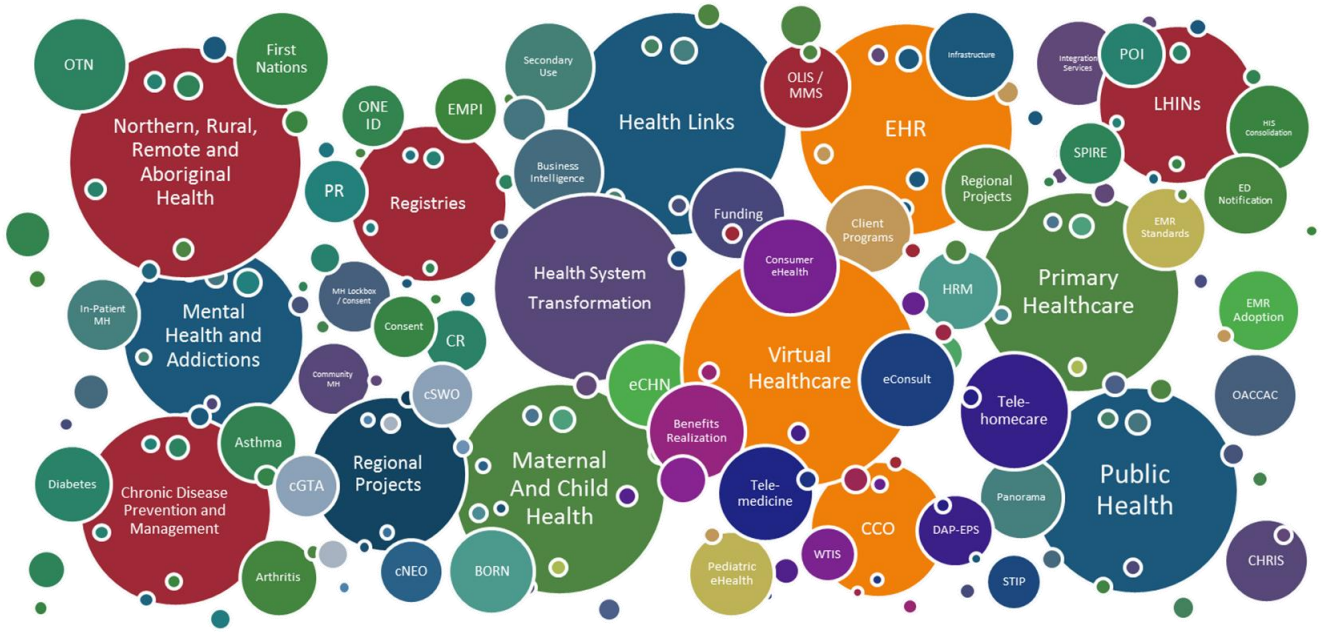
WHO, WHAT, WHEN, WHERE, WHY & HOW

OUTLINE

1. WHO - MANAGING COMPLEXITIES WITHIN THE SYSTEM
2. WHAT - CLINICIAN OBLIGATIONS
3. WHEN & WHERE - PRIMARY CARE & LARGER HEALTH CARE SYSTEM
4. WHY - SECONDARY USE
5. HOW - PROTECT THE DATA WITHIN YOUR PRACTICE

WHO?

MANAGING COMPLEXITY



THE LANDSCAPE: THE FLOW OF INFORMATION

Patient Tim

How information flows throughout the health care system is crucial to the care patients receive. When Tim visits Dr. Chris, he will disclose both personal health information (**PHI**) and personal information (**PI**) such as name, DOB and symptoms.

Dr. Chris

Dr. Chris will upload Tim's PHI and PI, onto her Electronic Medical Record (**EMR**). She may also use a variety of other digital health tools, which will assist her in providing Tim with care.

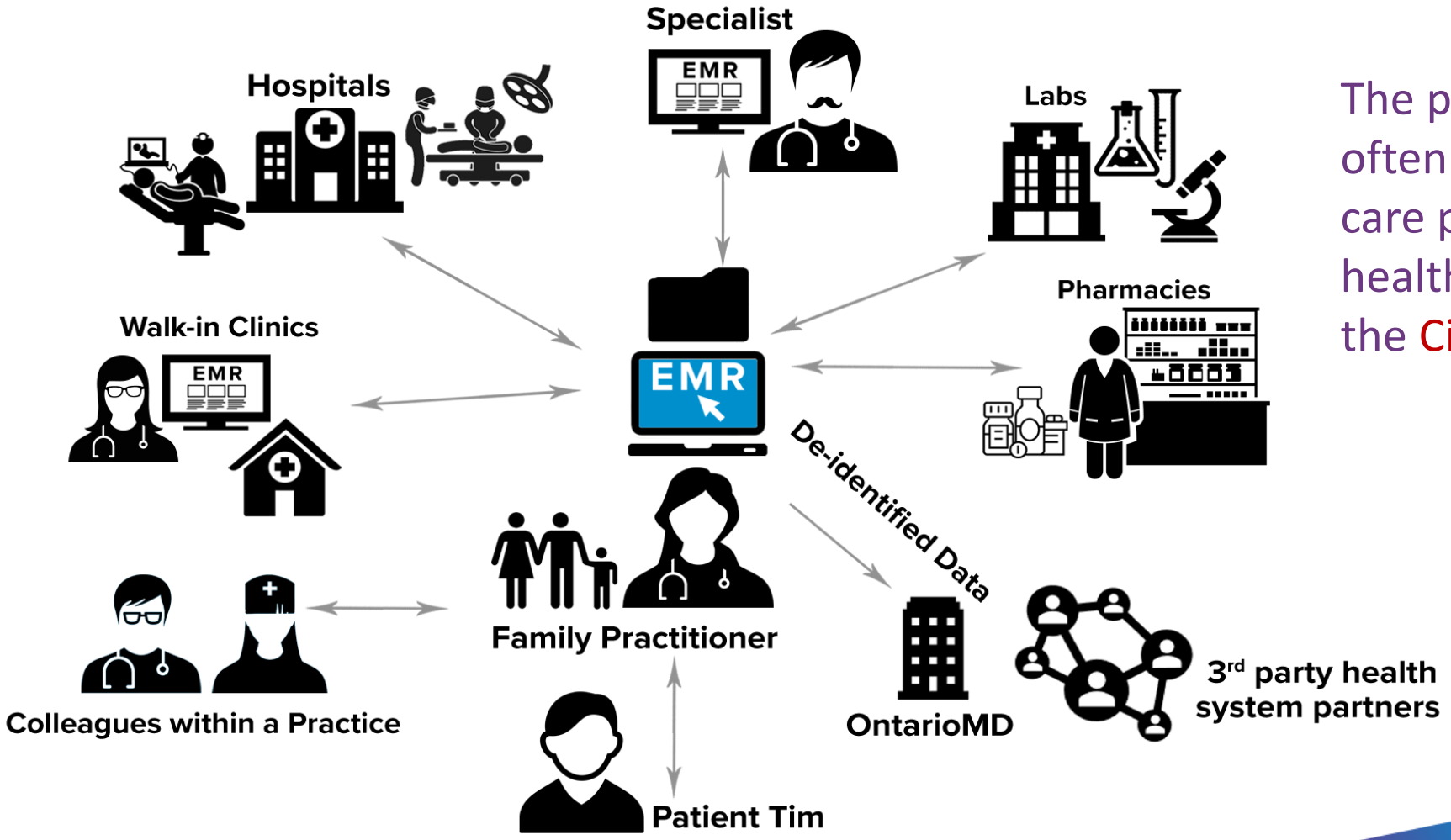
Dr. Chris' EMR + Digital Health Tools

HEALTH REPORT MANAGER

eNOTIFICATIONS

i4C DASHBOARD

FLOW OF INFORMATION THROUGH THE HEALTH CARE SYSTEM



The provision of care for a patient often extends beyond the primary care physician and involves other health care professions known as the Circle of Care

MEDICAL RECORD: WHO OWNS IT?

Clinician or Entity that created the Medical Record (i.e. hospital or clinic) owns the physical or digital medical record(s).

Medical records are understood to be in the shared custody and control of the clinician and the patient.

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

Exception - where there is a likelihood of harm to patient (IPC Decision 52).

WHAT?

WHAT

ARE THE CLINICIAN'S OBLIGATIONS?

RELEVANT LEGISLATION & REGULATIONS

Dr. Chris Health Information Custodian (**HIC**) their patient's PHI. While Tim's PHI is in her custody and control, she must protect Tim's privacy by safeguarding his data within her practice and the broader health care system.- TRUST

PRIVACY

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

OTHER

MEDICINE ACT
CPSO GUIDELINES
COURT ORDERS

KEY IPC HEALTH ORDERS

68

UNAUTHORIZED ACCESS – Hospitals must have adequate measures in place, such as audit logs to prevent unauthorized access to patient files.

74

DISCLOSURE - Clinicians must only disclose patient PHI to third parties with consent for permitted purposes such as administering care.

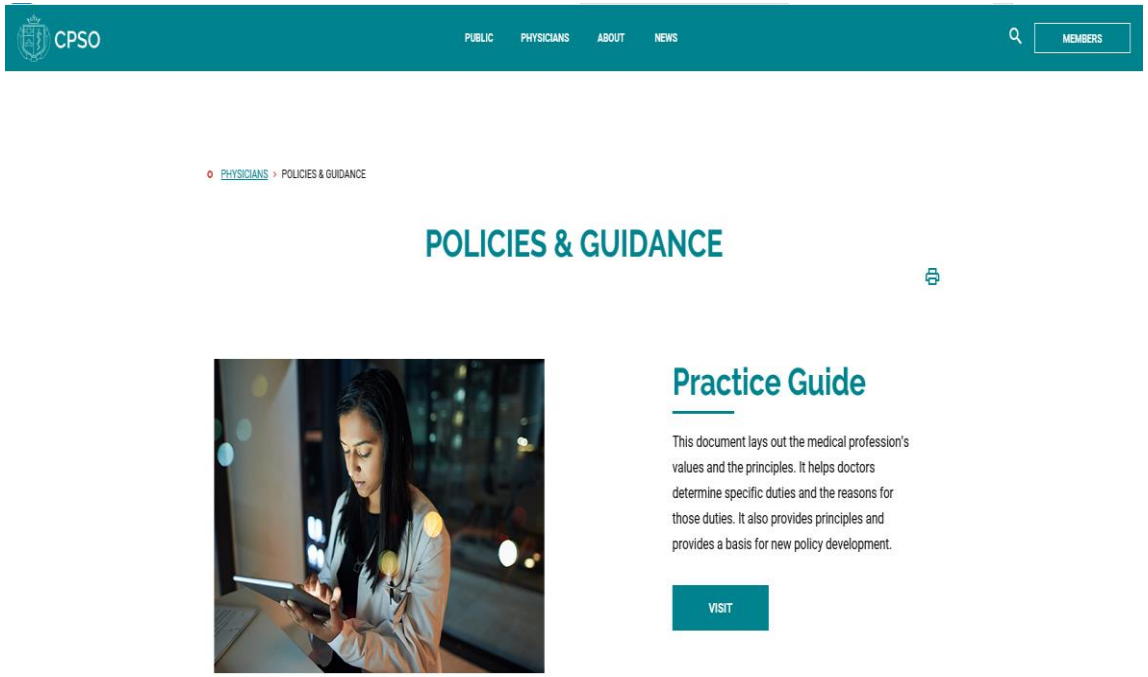
83

CONSENT – Children may expressly withdraw their consent to have any of their PHI disclosed to their parents.

CPSO – POLICIES

REQUIRMENTS

- The CPSO policies set out requirements and provide guidelines.



CLINICIAN OBLIGATIONS: SAFEGUARDING AND PROCESING PHI

COLLECTION & CONSENT

Dr. Chris must obtain consent prior to collecting and using Tim's PHI.

3 forms of consent:

Express
Implied
Assumed Implied

ACCESS/ USE

Dr. Chris owns the physical/digital health record **BUT** Tim has a right to reasonable access to examine and copy their records, **except** likelihood of harm to patient.

DISCLOSURE

Dr. Chris shall only disclose Tim's PHI when necessary for the provision of care.

⚠ HICs must consider what would the reasonable clinician do.

PRACTICAL TIPS FOR YOUR PRACTICE

Using a Certified EMR when collecting PHI is crucial to ensuring that patient information is adequately safeguarded.

EMR CERTIFICATION PROGRAM

Establish a Data Governance structure within you practice, set restrictions on who has access to what information. Dissolution of practice

IPC Decision 80 – DISCLOSING INFORMATION

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.

CLINICIAN OBLIGATIONS: SAFEGUARDING AND PROCESING PHI

RETENTION

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

Regardless of whether they are continuing to provide care to the respective patient(s).

Records must be securely stored and protected against theft, loss or unauthorized access.

RELOCATION

Transferring custody & control of patient records is governed by transfer & retention regulations. When transferring records electronically, it must be encrypted.

DESTRUCTION

Develop internal destruction policies, to ensure that PHI is completely removed from the practice.

MORE PRACTICAL TIPS FOR YOUR PRACTICE

ERASE electronic files with clearing software or hardware to overwrite sensitive data or purged. Paper Files should be disposed of in a separately marked bin and made indecipherable (e.g. cross-cut shredding).

Maintain updated patient enrolment and consent to release PHI. Patient files should include Record Transfer & Access Agreements.

- Patient should only be charged a modest fee to copy their record.

PUBLISH/POST Policies on Use of PHI

BACK UP YOUR SYSTEMS AND DATA. DOUBLE AND TRIPLE CHECK. Hire an IT Professional to help maintain all IT needs within your practice. Consider hiring a reputable company to provide safe and secure paper and electronic PHI disposal.

DATA SHARING

Dr. Chris wants to onboard new technology and is looking to sign an agreement with an external health care vendor, what are her obligations?

PROCESSING DATA

A Clinician can appoint a third-party agent to process data that includes PI/PHI (subject to administrative, physical and technological safeguards) but [the Clinician (or the Clinic)] must provide notice to [patients], and they are still responsible and accountable for what happens to that PI/PHI.

- **Sign a Non-Disclosure Agreement** with your external vendor, limiting what they can do with the data they encounter from your EMR.
- **Do Not** use patient data for secondary purposes without consent.

WHEN?/WHERE?

RELATIONSHIP BETWEEN THE PRIMARY CARE CLINICIAN & THE LARGER HEALTH CARE SYSTEM

Primary care clinicians, such as Dr. Chris, have always worked with other health care providers to administer care. Recently the Ontario government has commissioned the creation of Ontario Health Team(s) ("**OHTS**"). The goal is to improve the administration and integration of care. PHI must be able to follow patient Tim as he moves through health care system.

USE OF DIGITAL HEALTH TOOLS

As Dr. Chris administers care to Tim, a variety of digital health tools are made available to her. If she opts not to use ConnectingOntario ClinicalViewer and missing important information within Tim's file could be found liable?

- What would a reasonable clinician do in the circumstances? Important to use tools likely to impact how one administers care. DHDR/DHIR where available

HEALTH REPORT MANAGER

CONNECTINGONTARIO CLINICALVIEWER BUNDLE

INSIGHTS4CARE i4C

OLIS DEPLOYMENT

eNOTIFICATIONS

DHDR / DHIR EMR INTEGRATION

PRIVACY AND SECURITY TRAINING AND RESOURCES

eCONSULT DEPLOYMENT AND EMR INTEGRATION

FIELD QUESTIONS

AUDIT LOGS

Is there an expectation for an EMR to generate an audit log for searches?

- YES, electronic information systems, [must] implement the measures necessary to ensure that the [practice/hospital] is able to audit all instances where agents access PHI on its electronic information systems, including the selection of patient names on the patient index, [even if the entire medical record is not accessed]. – DECISION HO-013

DATA COLLECTION

A clinic is seeking to onboard technology to assist with booking patient appointments. The digital solution collections information related to the booking as well as additional PHI & PI that is not directly related to booking the appointment. If a clinician onboards that solution, are they violating PHIPA?

WHY?

THE IMPORTANCE OF PROTECTING DATA

OTHER SECONDARY USES

HEALTH CARE RESEARCH

Can Dr. Chris use the data in her EMR for research purposes? Does she need consent? If the data is de-identified does, she still need consent?

Any research involving PHI must be done in accordance with PHIPA. Dr. Chris must obtain Tim's consent when using data for research. Research must be approved by a research ethics board.

OTHER SECONDARY USES

INNOVATIVE USES – GRAY ZONE

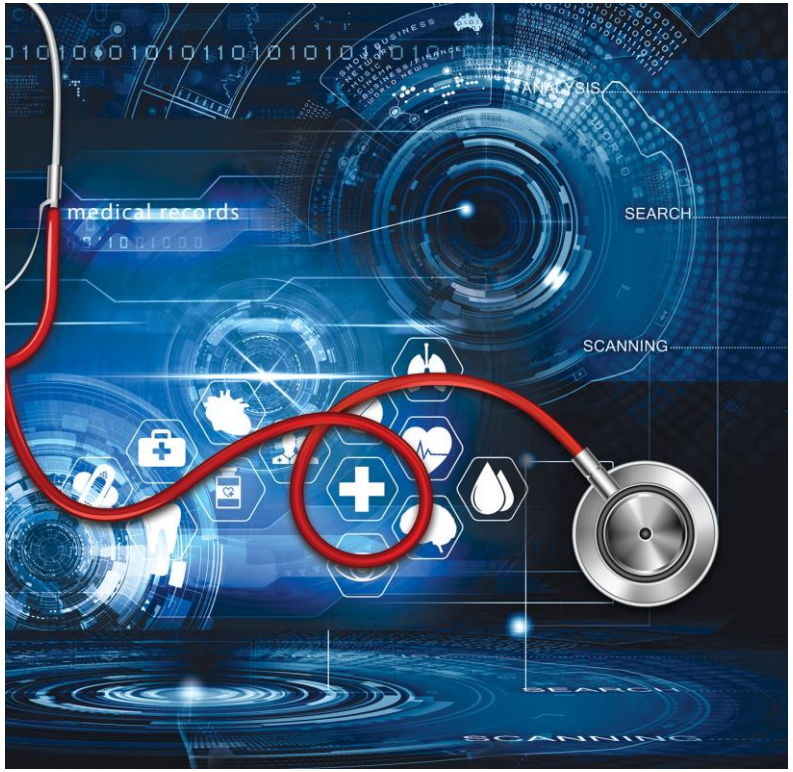
When it comes to innovative uses of PHI such as for AI the rules are less clear. Clinicians must ensure that they use best practices, such as obtaining express consent to use PHI for secondary uses.

The use of de-identified information in AI technologies may still be considered PHI. Always best to notify patients that their de-identified data may be used in this way (e.g. i4C Dashboard).

British Columbia v. Philip Morris International, Inc. – the law is NOT clear

HOW?

HOW TO PROTECT THE DATA WITHIN YOUR PRACTICE



CREATE AN ACCOUNTABLE PRACTICE

PRACTICAL TIPS FOR DATA PROTECTION

TRAINING

IPC Decision 64 – Annual Online Privacy Training Course for its agents.

Launch Privacy and Security Training Now

IMPLEMENT SAFEGUARDS

- Updated software and hardware (i.e. operating system, firewalls etc.)
- Encryption – at rest and in transit
- Transmit PHI through encrypted messages
- Two-factor authentication
- Have audit Logs
- **BACK UP**

DON'T DO IT ALONE, GET HELP!

PRIVACY POLICIES

RESPONSE PLAN

CYBERLIABILITY INSURANCE

MANAGE A BREACH

1. IDENTIFICATION
2. INTERNAL REPORTING
3. CONTAINMENT
4. NOTIFICATION
5. INVESTIGATION
6. REMEDIATION

SCENARIO: Dr. Chris' files have been locked and a hacker has requested that she pay $100,000 ransom for their release. What should Dr. Chris do?

ONTARIOMD PRIVACY & SECURITY TRAINING

ANYTIME, ANYPLACE, ANY DEVICE

OntarioMD's Privacy and Security Training Module is a comprehensive and complimentary training Module that is suitable for clinicians and staff alike. The Module will teach you about privacy and security fundamentals such as how to manage a data breach. Physicians also receive 2 Mainpro+ credits for completing the Module. Access the Module at https://www.ontariomd.ca.

Questions & Discussion

Ariane.Siegel@OntarioMD.com

THANK YOU !

ontariomd.ca

@ontarioemrs

OntarioMD

OntarioMD

OntarioMD

Ontariomd.blog