



# THE 2017 LEGAL GUIDE TO PRIVACY & INFORMATION MANAGEMENT IN HEALTHCARE

Having a clear understanding of current privacy laws in healthcare, your risks and how to manage them is critical....

Spend a day with Canada's leading health and privacy law experts who will use a case study approach to give you the knowledge and tools your organization needs including:

- Common causes of personal health information privacy breaches
- Understanding the role of a health information network provider (HINP)
- Knowing when to disclose personal health information to reduce or eliminate a "significant risk of serious bodily harm"
- Unique privacy challenges for the community health organization
- What steps do you take to contain and investigate a breach?

**Keynote Speaker:** Brian Beamish, Commissioner, Office of the Information and Privacy Commissioner of Ontario — *"Update from the IPC"*

Register today at:

[osgoodepd.ca/privacy-health](http://osgoodepd.ca/privacy-health)

## Program Chairs:

Mary Jane Dykeman,  
DDO Health Law

Lonny J. Rosen,  
Rosen Sunshine LLP

## Program Details:

DATE AND TIME:

April 10, 2017

9:00 a.m. - 4:15 p.m. EDT

In Person or Webcast

Online Replay: May 15, 2017

LOCATION

Osgoode Professional  
Development

1 Dundas St. West, 26th Floor  
Toronto, ON

# The 2017 Legal Guide to Privacy & Information Management in Healthcare

Privacy breaches can result in significant reputational risk, regulatory investigations and costly litigation. Recent high profile cases dealing with personal health information highlight how critical this issue has become for healthcare professionals and organizations.

If you are a healthcare risk manager, privacy officer, director of care/professional practice, lawyer advising on privacy and information management issues, nurse or nurse educator, allied health professional or other healthcare worker, you must have a current understanding of the key issues and how to deal with them.

It has never been more critical to be on top of the latest developments including:

- When can personal health information be used or disclosed in a proceeding? What rules apply?
- Understanding privacy impact assessments and threat risk assessments
- The rules respecting the collection, use and disclosure of personal health information
- What questions do you ask upon discovering a privacy breach has occurred?
- What are the risks health care providers face regarding privacy?
- The interplay of the *Mental Health Act* and *PHIPA* with respect to proceedings involving a patient in a psychiatric facility

## Who Should Attend?

- Privacy officers and other privacy professionals working in healthcare settings
- Family health teams
- Healthcare risk managers
- Directors of professional practice
- Directors of care
- Nurses; nurse educators; unit administrators; managers
- Allied health professionals
- Directors/VP's of nursing
- In-house counsel
- Lawyers advising on privacy issues and information technology
- Marketing and communications executives in healthcare

### What attendees said about the previous program

“Excellent and timely information concisely presented by knowledgeable experts.”

“A nice cocktail of relevant privacy & IM issues. Opportunity for questions & discussion highly valuable.”

## Agenda

**8:30 a.m.**

**Registration and Continental Breakfast**

**9:00 a.m.**

**Welcome and Case Study Introduction from the Chairs**

**Mary Jane Dykeman**, DDO Health Law

**Lonny J. Rosen**, Rosen Sunshine LLP

To prepare you for the day's sessions, the Program Chairs will present a complex fact scenario that will be woven throughout the day's presentations. This will bring the issues to life and give you an opportunity to see how privacy might actually play out in your organization.

This case study will get you thinking about some of the key issues that will be discussed throughout the day, including:

- What risks do health care providers face regarding privacy?
- What preventative steps should all providers be taking?
- What steps should be taken upon notification of a breach?
- When can personal health information be shared to prevent a risk of harm, and what information should be shared in these circumstances?
- When can personal health information be used or disclosed in a proceeding? What rules apply?

**9:15 a.m.**

**2017 Update on Strategies and Best Practices for Responding to and Managing Privacy Breaches in Healthcare**

**Sherry Liang**, Assistant Commissioner, Tribunal Services, Information and Privacy Commissioner of Ontario

- What you need to watch out for: the most common causes of personal health information (PHI) privacy breaches
- What to expect when a breach occurs and you call the Information and Privacy Commissioner (IPC) of Ontario

- What's new from the IPC?
- Not just a hospital issue: a wakeup call for all healthcare organizations

**10:00 a.m.**

### Framework for the Provincial Health Record Under Bill 119

**Manuela Di Re**, Director of Legal Services and General Counsel, Information & Privacy Commissioner of Ontario

This presentation will provide an overview of the legislative framework for the provincial electronic health record outlined in Bill 119, the *Health Information Protection Act*, 2016, including:

- The governance model
- The rules respecting the collection, use and disclosure of personal health information
- Consent directives and consent overrides
- Breach notification

**10:45 a.m.**

### Refreshment Break

**11:00 a.m.**

### Understanding the Role of a Health Information Network Provider

**Mary Jane Dykeman**, DDO Health Law

- What is a health information network provider (HINP)?
- What to ask for if you are a HINP
- What to ask for if you are a health information custodian working with a HINP
- Brief primer on privacy impact assessments and threat risk assessments (required of HINP's)

**12:00 p.m.**

### Luncheon (and Keynote Address)

**Brian Beamish**, Commissioner, Office of the Information and Privacy Commissioner of Ontario

*"Update from the IPC"*

**1:00 p.m.**

### Disclosing Personal Health Information in Proceedings: If, How and When?

**Lonny J. Rosen**, Rosen Sunshine LLP

- Review of *PHIPA* provisions that permit disclosure of PHI in proceedings: when and under what circumstances?
- Obligations and limitations of the parties in various proceedings to disclose PHI including in civil litigation and family law matters and WSIB complaints
- Interplay of the *Mental Health Act* and *PHIPA* with respect to proceedings involving a patient in a psychiatric facility
- Analysis of issues counsel may face in disclosing PHI
- Review of recent case law where PHI records were sought & the outcomes: professional regulation, medical malpractice, tort law, labour law, class actions

**1:45 p.m.**

### Analyzing the Risk of Harm Exception Permitting Disclosure of PHI

**Lad Kucis**, Gardiner Roberts LLP

- When should you disclose PHI to reduce or eliminate a "significant risk of serious bodily harm"?
- Knowing your obligations: What should you disclose? To whom? By what method?
- Teaching staff to use *PHIPA* provisions carefully - privacy should never cost lives
- What should be documented?

**2:30**

### Refreshment Break

**2:45 p.m.**

### Investigating and Responding to Privacy Breaches

**Adam Kardash**, Osler, Hoskin & Harcourt LLP

The privacy officer of a health care provider is advised by a staff member that a major privacy breach has occurred. Here are the

questions that need to be asked that will guide the privacy officer's actions:

- What is the privacy officer's first step?
- What considerations drive next steps?
- When should you call the Information and Privacy Commissioner of Ontario?
- What steps can be taken to contain and investigate the breach?
- Who should be notified, how and when?
- What other steps should be taken?

**3:30 p.m.**

### Privacy & Protection of PHI in Community Health Settings

**Bosco Chan**, Chief Privacy Officer, Ontario Association of Community Care Access Centres

**Anna Tersigni Phelan**, Privacy Officer, Canadian Mental Health Association, Waterloo Wellington

**Rodney Burns**, Chief Information Officer, Association of Ontario Health Centres

This session will review privacy and information management concerns specific to community health organizations, including:

- What do recent developments and recent changes to *PHIPA* mean for privacy protection in the community setting?
- Management of PHI: unique challenges and strategies for the community health team
- Strategies and tools for detecting and deterring privacy breaches
- What lies ahead? Areas of focus for change

**4:15 p.m.**

### Program Concludes

## Chairs

Mary Jane Dykeman  
DDO Health Law

Lonny J. Rosen  
Rosen Sunshine LLP

## Keynote Speaker

Brian Beamish, Commissioner, Office of the Information and Privacy Commissioner of Ontario

*"Update from the IPC"*

## Faculty Includes

Rodney Burns  
Chief Information Officer,  
Association of Ontario  
Health Centres

Bosco Chan  
Chief Privacy Officer, Ontario  
Association of Community  
Care Access Centres

Manuela Di Re  
Director of Legal Services  
and General Counsel,  
Information & Privacy  
Commissioner of Ontario

Adam Kardash  
Osler, Hoskin & Harcourt LLP

Lad Kucis  
Gardiner Roberts LLP

Sherry Liang  
Assistant Commissioner,  
Tribunal Services,  
Information and Privacy  
Commissioner of Ontario

Anna Tersigni Phelan  
Privacy Officer, Canadian  
Mental Health Association,  
Waterloo Wellington

## Registration Details

### Fee per Delegate

**\$525 plus HST**

Fees include attendance, program materials, continental breakfast, lunch and break refreshments. Group discounts are available. Visit [www.osgoodepd.ca/group-discounts](http://www.osgoodepd.ca/group-discounts) for details. Please inquire about financial assistance.

### Program Changes

We will make every effort to present the program as advertised, but it may be necessary to change the date, location, speakers or content with little or no notice. In the event of program cancellation, York University's and Osgoode Hall Law School's liability is limited to reimbursement of paid fees.

### Cancellations and Substitutions

Substitution of registrants is permitted at any time. If you are unable to find a substitute, a full refund (less \$75 administration fee) is available if a cancellation request is received in writing 14 days prior to the program date. No other refund is available.



OsgoodePD has been approved as an Accredited Provider of Professionalism Content by the LSUC.



Eligible CPD/MCLE Hours: LSUC (ON): 6.75 CPD Hours (5.75 Substantive, 1.0 Professionalism)

OsgoodePD programs may be eligible for CPD/MCLE credits in other Canadian jurisdictions. To inquire about credit eligibility, please contact [cpd@osgoode.yorku.ca](mailto:cpd@osgoode.yorku.ca)



The presentation, The 2017 Legal Guide to Privacy & Information Management in Healthcare, is eligible for 7.0 CHIMA CPE credits.



CANADIAN COLLEGE OF  
HEALTH LEADERS  
COLLÈGE CANADIEN DES  
LEADERS EN SANTÉ

Maintenance of Certification  
Attendance at this program entitles certified Canadian College of Health Leaders members (CHE / Fellow) to 3 Category II credits towards their maintenance of certification requirement.

[osgoodepd.ca](http://osgoodepd.ca) **Osgoode Professional Development**  
 **416.597.9724** **1 Dundas Street West, Suite 2600**  
 **@OsgoodePD** **Toronto, ON Canada M5G 1Z3**



## The 2017 Legal Guide to Privacy & Information Management in Healthcare

Register today at:

[osgoodepd.ca/privacy-health](http://osgoodepd.ca/privacy-health)