Health Sector Privacy Officer Training – Full Details and Learning Objectives
Spring 2016 - 3 Full Days
Dates April 12, May 10, and June 14

The privacy practices of health care organizations and providers are under increasing scrutiny from your patients, residents or clients (and their families), the courts, the media and the Information and Privacy Commissioner of Ontario (IPC/O). Attorney General prosecutions are underway under the *Personal Health Information Protection Act* (PHIPA), and class actions have been filed in the courts. On September 16, 2015, Bill 119, the *Health Information Protection Act,* was introduced. If passed it will double the fines under PHIPA to up to $100,000 for individuals and $500,000 for organizations and require reports to the IPC/O of certain privacy breaches and reports to regulatory Colleges, among other changes.

This is the only course of its kind in Canada. **While we focus on Ontario legislation – this course is of value to any health sector Privacy Officer.** It will give you confidence in your role by giving you the information and skills you need to succeed as a Privacy Officer. You receive:

- 20 hours of intensive instruction from leading legal educators in the field
    - 3 full day sessions each available in person in downtown Toronto or via webcast
- Reassurance that you have the most current information on privacy practices and expectations for health care organizations
- Practical and dynamic skills training for adult learners using scenarios, stories, quizzes and assignments
- Sample tools to adapt to your organization for your everyday use, including:
    - Privacy program checklist
    - Privacy program documentation checklist
    - Privacy policies
    - Annual confidentiality pledge for all staff, students and volunteers
    - Privacy communiques
    - Board update on privacy
    - Privacy impact assessment
    - Privacy breach checklist
    - Privacy breach notification
- A privacy library
    - The primary Ontario privacy resource – "Guide to the Ontario Personal Health Information Protection Act: A Practical Guide for Health Care Providers" (H. Perun, M. Orr, F. Dimitriadis, Irwin Law, 2005)
    - Online resources are compiled for you in a few downloadable PDFs so you do not have to find the resources yourself and print them individually
- A reading list to prepare you before each session
- Homework to assist you to work through your own organization's documents
- A report card you complete yourself at the end of the course to share with your Board or supervisor to demonstrate your organization's privacy compliance status and remaining privacy gaps, if any
- A letter outlining the training you have received, for your organization's due diligence

Day 1 –April 12, 2016

Session 1: The Privacy Basics

Are you new to the role of Privacy Officer? Are you new to the health care sector? Do you need a refresher on privacy laws for health care organizations? This session provides an overview of Ontario's health privacy law (the *Personal Health Information Protection Act, 2004* – PHIPA) and the privacy basics and terminology.

By the end of this session you will be able to:

- Understand basic privacy terminology such as: personal health information (PHI); health information custodians (HICs); agents; collection, use, and disclosure; circle of care, lockbox; privacy impact assessments (PIAs); and threat risk assessments (TRAs)
- Explain the rights individuals have to privacy
- Identify the basic "consent rules" of privacy and the exceptions to those rules
- State the situations where your organization can collect, use and disclose PHI with and without consent
- Understand the role of the IPC/O
- State the possible consequences for privacy breaches and poor privacy practices with knowledge of current cases and referrals for prosecution

Session 2: Privacy Compliance Overview

This session reviews the key sources of the privacy laws and rules, the duties of a HIC, the role of the Privacy Officer and the tools you will need to do your job. It also provides you with sample policies and patient communiques to jumpstart your privacy compliance efforts whether your own policies are limited or outdated.

By the end of this session you will be able to:

- Identify the 7 main sources of the privacy laws, rules and best practices in Ontario
- Use our 15 point Privacy Program Checklist to evaluate how well your organization is doing with its own privacy compliance and present an update to your Board
- Articulate a strategy for your organization's privacy program launch or refresh
- Organize your privacy binder/electronic folder by using our Privacy Program Documentation Checklist

Session 3: Creating and Reinforcing a Culture of Privacy

In this session you learn the IPC/O's expectations and best practices for how to create and reinforce a culture of privacy.

By the end of this session you will be able to:

- Launch or refresh your orientation program for new staff, students and volunteers to include:
    - Privacy policies (samples provided)
    - All staff training (in-house training is an optional extra service option we can provide to you)
    - Confidentiality pledge (sample provided)
    - Board training (PowerPoint provided)
- Launch or refresh your privacy program to include:
    - Timelines for updating privacy policies
    - Schedule for annual training
    - Annual confidentiality pledge (sample provided)
    - Email reminders/newsletters to all staff on a regular basis (subscription is an extra service option available to receive monthly emails to send to all staff)
    - Follow up with all staff if there is a privacy breach
    - Random audits (messaging to staff, frequency and scope)
- Respond to common challenges in engaging staff, physicians, students and volunteers

Day 2 –May 10, 2016

Session 1: Security and Safeguards

In this session you learn how to approach health privacy security issues and the safeguards you should have in place. By the end of this session you will be able to:

- Identify the 3 categories of safeguards: physical, administrative, and technological; and the common examples of how to protect the PHI you hold
- Read and understand a PIA and TRA
- Determine when you can conduct your own and when to solicit an external PIA or TRA
- Conduct random audits of an electronic health record system and identify suspicious activity
- Identify and respond to the areas of greatest risk for health care organizations

Session 2: Consent, Circle of Care and Lockbox

In this session we discuss the concept of consent and the choices individuals can make about their health care information. We also discuss the concepts of the "circle of care" (that is, sharing information with other health care providers for health care purposes relying on implied consent) and "lockbox" (that is, a patient's choice to restrict relevant health information from health care providers for health care purposes).

By the end of this session you will be able to:

- Differentiate between express consent, implied consent and no consent
- Understand the difference between consent and notice
- Understand who can make substitute decisions and under what circumstances (especially for young children, incapable adults or deceased persons)
- Have a conversation about integrating "consent management" into your electronic systems
- Explain the circle of care to patients and staff
- Identify the key opportunities and issues of concern with shared care models (such as HealthLinks)
- Explain a lockbox to patients and staff (brochure and information sheet provided)
- Identify what a lockbox looks like in an electronic health record
- Provide sample language to your clinicians for communicating with external health care providers when there is a lockbox restricting disclosure

Session 3: Secondary Uses and Disclosures

In this session you learn about the secondary uses and disclosures you can make with health information without the consent of patients. You will also learn about data sharing agreements and the special rules that apply if you are a Health Information Network Provider (HINP), or if you are engaging a HINP.

By the end of this session you will be able to:

- Explain to patients and staff when you need patient consent to engage in an activity and when you do not
- Strategize within your own organization about who is authorized to engage in secondary uses and disclosures – and who is not
- Identify the key opportunities and issues of concern when participating in large health sector quality, efficiency and reporting initiatives
- Understand the key elements of a data sharing agreement
- Identify a situation when you are being asked to be a HINP and understand the responsibilities of fulfilling that role and potential consequences of failing to meet those responsibilities

Day 3 –June 14, 2016

Session 1: Access, Correction and Disclosure to Third Parties

In this session we explain the rights and limits to patients accessing and asking for a correction to their own PHI. We also review common situations where third parties ask for copies of health records or access to patient databases.

By the end of this session you will be able to:

- Process simple access and correction requests (and identify situations where you need expert advice)
- Address individual requests for access to "family records" where there is a single record for multiple patients (e.g. in some counselling settings, or in situations where information about a newborn remains in the mother's record)
- Identify key situations where your organization is required by law to disclose PHI (mandatory disclosures)
- Avoid an order for deemed refusals of access
- Respond to common complicated situations in third party disclosure, with or without consent:
    - Parents
    - Insurance companies
    - Lawyers and courts
    - Regulatory bodies: Workplace Safety and Insurance Board, College of Physicians and Surgeons of Ontario and other health regulatory Colleges
    - Ministry and health sector partners (for anonymized data)
    - Police
    - Children's aid societies

Session 2: Privacy Breach Investigation and Response

In this session we complete two case studies of privacy breach investigations. It includes a 10-part checklist of what you must have in place to emerge well from a privacy breach.

By the end of this session you will be able to:

- Conduct your own privacy breach investigation
- Determine when to ask for an external investigator to complete an investigation
- Notify affected patients in the case of a privacy breach
- Write a privacy breach report
- Anticipate how to work with the IPC/O
- Manage common questions from the media
- Determine the level of detail to share with other staff not involved in the breach
- Determine the appropriate disciplinary consequences for a privacy breach

Session 3: Recent Developments

Winter/Spring 2016 promises to be a very busy with changes to the privacy landscape. In this session we advise you of the latest developments in IPC/O orders, status of class action lawsuits, referrals to the Attorney General for prosecutions of privacy breaches under PHIPA and possible introduction of PHIPA amendments.

By the end of this session you will be able to:

- Feel confident that you understand the most recent updates to privacy laws and rules
- Update your policies and privacy practices to reflect these new developments

Session 4: Questions and Answers

In this session, we highlight common scenarios and answer your questions. Time permitting, we will also highlight some tips for building privacy into your website functionality, including terms and conditions and user registration.

COST PER REGISTRANT

Regular price for The Privacy Officer Training program	$2900 + HST
Super Early Bird (register before January 31, 2016)	$2500 + HST
Early Bird (register before March 1, 2016)	$2600 + HST

Group discounts:

- Group of 5-9 organizations $2200 + HST each (please list group members on your form)
- Group of 10+ organizations $1975 + HST each (please list group members on your form)

Fees include course attendance, continental breakfast, lunch, refreshment breaks and course materials. Webcast fees are per individual participant. Please ask about further group rates for multiple registrants from the same organization.

LOCATION

St. Andrew's Club and Conference Centre at 150 King St W in Toronto, ON (King St. W. and University Ave.) http://www.standrewsclub.ca/ (Or via webcast)

DDO Health Law

DDO Health Law is Canada's leading law firm in health law education. The training is provided by Mary Jane Dykeman and Kate Dewhirst. We bring experience, humour and vitality to each training session. We work with health care organizations across the continuum of care (from primary to quaternary care, community and social services, academic centres, as well as children's, seniors' and mental health and addiction providers). We know the common and complex issues Privacy Officers face and the scenarios that will resonate with you.

Testimonials

Here's what previous registrants had to say about this course:

- *The instructors and team at DDO Health Law are healthcare privacy experts and this course is a valuable resource for all healthcare Privacy Officers. The training provided me the knowledge to transition into my new role confidently.*
- *I really appreciated the templates! As an ED who wears many hats, this was a huge time saver and plus gave me the relief that we have in place what we need now.*
- *The tools were excellent. We are developing a privacy framework in this LHIN with consultants but internally I also needed help to emphasize the importance of privacy.*
- *Liked it all, but what really made this course different was that the trainers are actually the subject matter experts and as such, questions could be answered in depth.*
- *The depth of knowledge and hands on experience of the trainers is what makes this training superb.*
- *The instructors were very knowledgeable and because it related to healthcare, very relevant. Was great to have feedback from other health organizations.*
- *Real life examples go a long way to proving how real privacy issues are and the consequences for them.*

TO REGISTER (complete information below):

Please email flatino@ddohealthlaw.com or fax to 416-967-7120

Name: _____ Title: _____

Organization Name: _____

Address: _____

Phone:_____ E-mail: _____

Attendance Options

□ In person
□ Webcast (fee per person)

Please specify dietary requests (if any):_____

Cost

□ Regular registration	$2900 + HST = $3277
□ Super Early Bird (before Jan. 31)	$2500 + HST = $2825
□ Early Bird (before Mar. 1)	$2600 + HST = $2938
□ Group of 5-9	$2200 + HST = $2373 (per organization per registrant)

List group members here: _____

_____

□ Group of 10+ $1975 + HST = $2231.75 (per organization per registrant)

List group members here: _____

_____

_____ _____

_____

Payment options

□ Cheque enclosed **(payable to DDO Management Inc. – HST #831543020RT0001)**
□ Bill my credit card – **VISA only**

Card #_____ Exp. _____

Name on card _____

Signature _____ Date _____

CANCELLATIONS, SUBSTITUTIONS & COURSE CHANGES

A substitute is welcome to attend in your place. Cancellations are accepted with refund (less a $60 administrative fee) up to 10 days prior to the event, otherwise no refund is available. Except that we do offer a confidence guarantee: If after attending the first day of the course you do not feel more confident as a Privacy Officer, we will refund your attendance fee. It may be necessary for us to change the date, venue, content and/or speakers with little or no notice. We will reimburse paid fees for course cancellation only, and we assume no further liability for course changes.