

Health Sector Privacy Officer Training 2017 Back by popular demand!

**June 6 (in person in downtown Toronto or via webcast, your choice) +
Weekly/biweekly teaching sessions, resources & online community to March 31, 2018
(your access begins upon registration, no need to wait until June)**

As health care organizations and providers, your privacy practices are under 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. Bill 119 amended PHIPA in numerous important ways (including doubling the fines to up to \$100,000 for individuals and \$500,000 for organizations and requiring reports to the IPC/O of certain privacy breaches and reports to regulatory Colleges).

This course focuses on Ontario legislation, but 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 or as:

1. A Chief Information Officer
2. A person with a Privacy Officer reporting to you, or
3. If you advise organizations that are subject to health privacy requirements or create related health policy

You receive:

- A full day session in downtown Toronto (or via webcast, the choice is yours) where we will launch the community and tackle some of the tough issues
- An additional weekly or biweekly set of webinars, videos, resources and intensive instruction from a leading legal educator in the field, most in real time
- **30+ hours (up from the original 3-day course of 20 hours)** with flexibility to learn at a pace that works for you, and with the support of a community
- 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 practical applications for your environment
- Sample tools to adapt to your organization for your everyday use, including these templates:
 - Privacy program checklist and document checklist
 - Privacy policies
 - Annual confidentiality pledge for all staff, students, volunteers and researchers
 - Privacy communiques (to customize and circulate as evidence of your due diligence)
 - Board update on privacy
 - Privacy impact assessment resources
 - Privacy breach checklist
 - Privacy breach notification/script
- 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 compiled for you, so you do not have to search them out yourself
- Strategies to assist you to work through your organization’s documents
- A report card you complete at the end of the course to share with your Board or supervisor to demonstrate your organization’s privacy compliance status and privacy priorities (or gaps, if any)
- A letter outlining the training you have received, for your organization’s due diligence

LOCATION – June 6, 2017 St. Andrew’s Club and Conference Centre at 150 King St W., 27th Floor, Room L2, Toronto, ON (King St. W. and University Ave.) <http://www.standrewsclub.ca/> (Or via webcast)

WHY DID WE CHANGE THE COURSE FORMAT?

Some of you have said that being out of the office three full days over three months was challenging, and/or that you welcome online opportunities, and that you love the community and problem-solving that comes with a membership. We have passed on that savings to you, and are pleased to offer new and interactive ways to learn where you get what you need.

COVE ACADEMY

Cove Academy is a new and innovative training platform. Our lead trainer in the course is Mary Jane Dykeman, a Principal of Cove Academy and lawyer at DDO Health Law. 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 exactly why PHIPA was drafted as it was, the nuance of PHIPA’s application within your environment, and the common and complex issues Privacy Officers and others working in privacy face daily. We have developed scenarios that will resonate with you.

WE WILL COVER:

1. Recent developments, risk management and due diligence (Full-Day session and throughout the course as new orders and decisions of IPC/O arise)	2. The privacy basics, including general limiting principles and collection rules	3. Privacy compliance overview	4. Creating and reinforcing a culture of privacy	5. Security & safeguards, including the ins and outs of audits and increasing number of shared systems
6. Consent and capacity in the PHIPA context	7. Secondary Uses and Disclosures	8. Disclosure to third parties	9. Who is the health information custodian?	10. Privacy breach investigation & response
11. IPC/O orders and decisions – what you need to know	12. How to create and show due diligence	13. Attorney General prosecutions – what we know so far	14. Dealing with the media	15. Tips for training staff whether you are a large or small health information custodian
16. Circle of care and lockbox	17. Access & Correction	18. Special rules related to children	19. Special rules in mental health settings	20. Q&A – What keeps you up at night?

**Overwhelmed? Don't know what you don't know?
By signing up for this course, you will confidently 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
- 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
- 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 (customizable 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
- Identify the 3 categories of safeguards under PHIPA: physical, administrative, and technological; and 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
- 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

- Strategize within your own organization about who is authorized to engage in secondary uses and disclosures – and who is not
- Explain to patients and staff when you need patient consent to engage in an activity and when you do 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 health information network providers and understand the responsibilities of fulfilling that role and potential consequences of not doing so
- 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, including:
 - 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 (including for anonymized data), Police, Children’s aid societies, requests for records to be brought to court and/or for evidence to be given (including the nuance for mental health records)
- 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
- Update your policies and privacy practices to reflect these new developments

Testimonials

Here’s what previous registrants had to say about previous versions of this course:

- *This seminar was hands down the best privacy seminar I have ever attended. AMAZING!*
- *The instructors and team . . . 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.*

TO REGISTER (complete information below)

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

Name: _____ Title: _____
 Organization Name: _____
 Address: _____
 Phone: _____ E-mail: _____

Attendance Options - June 6 session

- In person Please specify dietary restrictions (if any): _____
 Webcast (fee per person)

Registration Cost (pp) – *for fiscal year-end purposes, we can provide invoices dated for March 31st if you register by April 7, 2017*

- Regular price for the Privacy Training program** **\$1999 + HST**
 Early Bird (deadline May 1, 2017) **\$1699 + HST**
 Alumni Rate* **\$ 999 + HST**

*(*Privacy Officer Training Alumni rate is for the organizations who participated in any of our 2015 to January 31, 2017 Privacy Officer sessions. These organizations may send delegates to the full-day onsite or live webcast for \$999 (plus HST) and both the Alumni and the delegate(s) will receive access to online resources including the full-day webcast until March 31, 2018.)*

Fees include course attendance, course materials and electronic participation; on the full-day if joining in person, includes continental breakfast, lunch and refreshment breaks. Webcast fees are per individual participant. Please ask about further group rates for multiple registrants from the same organization.

Payment options

- Cheque enclosed **(payable to D&O Training Inc., Cove Academy's legal name)**
 Bill my credit card – **VISA and MASTERCARD**

Name on card: _____ Exp.: _____
 Card #: _____
 Signature: _____ Date: _____



Cancellations, Substitutions & Your Satisfaction Guaranteed

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. We offer this confidence guarantee: If after attending the course and online resources, you can show us that you have diligently worked through the course content and resources and 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, with no liability for course changes. We are really excited you will join us and that you will feel more confident in your role. See you there!