Kate Dewhirst
BRINGING THE LAW TO LIFE

The Privacy Prescription for Health Care Practices

Health care practices of all shapes and sizes need a strategy to deal with compliance with the *Personal Health Information Protection Act, 2004* (PHIPA).

With privacy compliance there are 11 basic steps your health care practice should ensure are managed.

I'd love to work with you on some or all of these steps. Just depends on what you've already accomplished.

I do most of my privacy work for a flat rate so you know exactly what it will cost. Email me: kate@katedewhirst.com

Step 1: Identify the Health Information Custodian

Step 1 is sorting out who is the "Health Information Custodian" for purposes of PHIPA. Basically – who "owns" the record and who is responsible for compliance with PHIPA. Depending on your practice this may be obvious (hospital, long-term care home, sole practitioners and community health centres) or complicated (group practices and family health teams). This analysis can depend on:

(1) Your type of health care practice;
(2) The agreements between the clinicians and the Ministry of Health and Long-Term Care or LHIN;
(2) The agreement between the group of clinicians (if any);
(3) Who owns the electronic health record.

Solution Available for Purchase: If you operate a group practice that is not listed as a custodian under PHIPA, you may need a PHIPA agreement. I can provide that for you and guide your decision making.

Step 2: Choose a Privacy Officer

There are five things a privacy contact person must do and 17 other things a privacy officer usually does. Read more here.

Step 3: Communicate

You need to advise your patients, residents or clients of their privacy rights. There are free posters and brochures available through the Information and Privacy Commissioner of Ontario.

- Health Information Privacy in our Office - Poster
- Health Information Privacy in our Hospital - Poster
- Health Information Privacy in our Facility - Poster

Solution Available for Purchase: I can give you a user-friendly public privacy policy that you can use to post on your website that explains your privacy practices. And we can edit your orientation materials to explain privacy.

Step 4: Policies

You need the following policies (or at least content in your policy):

- Consent and capacity
- Safeguards (deals with ransomware, email, phone, off site transportation issues, texting)
- Breach protocol
- Privacy Impact Assessment

- Lockbox
- Access and Correction

Solutions Available for Purchase: If you are in Ontario only and your policies mention the *Personal Information Protection and Electronic Documents Act* (PIPEDA) – you likely need brand new policies (not always – but that reference is a good sign your policies may be out of date or refer to legislation that does not apply to you). If your policies say you ONLY ever rely on express consent – you likely need new policies. I have a package of privacy policies that you can easily edit to your unique circumstances. Or – if you have good privacy policies already, I can review your existing privacy policies for you at a flat rate to make sure they are up-to-date regarding ransomware, social media and privacy notification requirements. We can discuss what works best for you.

Step 5: Staff Training

Under PHIPA, the health information custodian is required to train all its staff and "agents" (meaning ANYONE who touches or deals with the health records on behalf of the custodian) about privacy and the custodian's privacy policies and expectations. This should be done **formally** every 3-4 years and there should be a plan of action for reminding staff and agents about privacy issues in an ongoing way (like email privacy updates from the Privacy Officer).

Solution Available for Purchase: I can provide your team with privacy training that is interactive, fun, and practical. I have taught more than 7800 people about health privacy. My most popular course takes 3 hours. I know that sounds like a long time – but I promise you, people will be engaged and it means they get all their questions answered. There is 1 hour of time dedicated to answering questions – and there will be a lot of questions.

For the formal training, I cover:

- Privacy terminology and privacy rules
- Consequences for a privacy breach – why does this training matter? What could it cost us if we don't do privacy well?
- Patient Rights
- Consent Rules and exceptions to the rules
- Circle of Care: Sharing information as part of a "health care system"
- Lockbox: Can patients decide not to share information with their health care providers?
- Social media and technology issues
- Third party requests for information (WSIB, CPSO, lawyers, police)
- Working within HealthLinks and other community sharing projects
- Privacy Standards & IPC Orders – storytelling to bring privacy to life

Here is one testimonial about this training:

I am a family physician working in a busy Family Health Team. PHIPA impacts all of our clinical and administrative activities. Kate Dewhirst provided us with an engaging and highly informative presentation. She was able to make a large room of multidisciplinary health care providers and administrative staff feel more like a small group session with lots of informal interactions, humor, questions and answers and real life examples of privacy issues and management. Kate kept the meeting on schedule and organized. Kate's information motivated me to make some immediate changes in my office function. I can highly recommend Kate Dewhirst as an excellent, high value resource in navigating the confusing waters of health care privacy.

Dr. Richard Wiginton, Brighton/Quinte West Family Health Team

I also have 1-hour training and 2-hour on-line privacy training for teams.

Step 6: Board Training

If you have a board, you should also train your board in privacy.

Solution Available for Purchase: I do a privacy session for board members to go over the obligations of the organization (different from the struggles of the front line staff members).

Step 7: Updating Contracts

You should look at your contracts with your vendors (especially your eHR provider, shredding contracts and off-site storage contracts as well as cleaning companies and others who come on site).

Solution Available for Purchase: I have PHIPA terms and conditions clauses for agreements with your vendors.

Step 8: Conducting a Privacy Audit

First, you need basic compliance (by dealing with steps 1-7). You'll have a policy of how to do a privacy impact assessment and as part of that tool there is a self-assessment piece. But eventually, you will each need to do a privacy audit to see how your practices measure up. As part of that, you should have a privacy improvement plan with a prioritized list of ways to improve privacy within your organization and assigned deadlines.

Solution Available for Purchase: I can do privacy audits for you. And I have tools to help you do privacy compliance self-assessments.

Step 9: Responding to Privacy Breaches and Complaints

You'll have your privacy breach policy which you can follow. If you need any assistance with complicated complaints or breaches, I can coach you through those. I help dozens of health care practices with their privacy issues.

Solution Available for Purchase: Pretty much every day I coach health care practices to manage their privacy issues including responding to the IPC and media.

Step 10: Insurance

You should look into cyber risk insurance for your organization. There is specific insurance you can get for privacy breaches.

Step 11: Report your privacy statistics and trends

You'll want to set up a reporting structure so your board, or leadership, know what kinds of privacy issues you are managing on a yearly basis. And as of January 1, 2018 you have mandatory tracking and reporting to the IPC.

Resources:

You might want to look into getting some privacy resources for your Privacy Officer:

- IPC website www.ipc.on.ca for Orders/Decisions, Fact sheets, Brochures, Practice Directions
- College guidelines and practice standards
- Free OHA/OMA Hospital Privacy Toolkit
- Free Mental Health Sector Toolkit

Here is a free summary of the IPC's 60 orders and decisions – current to November 28, 2017

I am launching Privacy Officer training again in May 2018 – I've trained more than 200 health privacy officers. Advanced Privacy Officer training launches for the first time January 16, 2018.

You can check out my blog at www.katedewhirst.com – you can filter for "privacy"