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 (sole practitioners, community health centres, hospitals) or complicated (group practices and family health teams and municipalities). This analysis can depend on:

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

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 or clients of their privacy rights, your information management practices and how to contact your privacy contact person. There are free versions of such posters available through the Information and Privacy Commissioner of Ontario such as: Health Information Privacy in our Office - Poster

Step 4: Policies

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

- Safeguards (deals with audits, ransomware, virtual care, working from home, email, phone, off site transportation issues, texting, paper records)
- Breach protocol
- Patient access to their own records and how to make correction requests for records
- Consent and capacity – who makes decisions for incapable patients and when do children decide
- Lockbox or consent directives
- Storage and retention of health records

Step 5: Staff Training

Under PHIPA, the health information custodian is required to train all your 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. Every year you should have some privacy training/communications to your team with more formal detailed privacy training every 3-4 years.

Step 6: Board Training

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

Step 7: Update Contracts

You should look at your contracts with your vendors (especially your electronic health record provider, shredding contracts and off-site storage contracts as well as cleaning companies and others who come on site) to ensure you are protected from their activities with your health records or information about your patients.

Step 8: Conduct a Privacy Inventory and Audit

First, you need basic compliance (by dealing with steps 1-7). But eventually, you will each need to do a privacy inventory of the personal health information you hold and an audit to see how your privacy 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.

Step 9: Respond to Privacy Breaches and Complaints

You need a privacy breach policy which you can follow if there is a breach or you receive a complaint. Make sure to manage (1) containment; (2) reporting to the Information and Privacy Commissioner and others; (3) notification of affected individuals and partners; (4) investigation; and (5) remediation. Follow the Information and Privacy Commissioner guidelines on responding to a health privacy breach.

Step 10: Insurance

You should look into cyber risk insurance. There is specific insurance you can get for privacy breaches and out of pocket expenses relating to notification of affected patients, damages to patients, equipment impact and other risks.

Step 11: Report your privacy statistics and trends

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

Privacy Officer Supports

Free "Ask me Anything about Health Privacy" webinars first Wednesday of every month (except over the Summer)

Free Summary of all the Information and Privacy Commissioner decisions on health privacy in Ontario

Health Privacy Officer Foundations training – next course starts September 2021

The Shush: a collective of health privacy officers membership and community