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 14 basic steps your health care practice should ensure are managed.

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, birth centres, 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. Details here.

Step 3: Make Records Available

You must make your health records available to clients including paper and electronic health records in an electronic format. There are exceptions to a client's right of access.

Step 4: Policies

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

- Safeguards (deals with audits, IT security, backups, ransomware, virtual care, working from home, email, phone, off site transportation issues, texting, paper records)
- Breach protocol
- Client access to their own records and how they make correction requests and how you respond to third party requests for records (CAS, WSIB, College, police, insurance etc.)
- Consent and capacity – who makes decisions for incapable clients 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 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. It is recommended you have all agents sign a confidentiality pledge annually.

Step 6: Communicate – Statement of Information Management Practices

You need to advise your 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: Your Health Information and Your Privacy

Step 7: Safeguards and Security

You must ensure the protection of personal health information you hold against loss, theft, unauthorized access, use or disclosure, copying, modification, disposal. This is through technical, physical and administrative safeguards. You must also conduct audits and privacy impact assessments and threat risk assessments to evaluate your security measures.

Step 8: Retention

You must ensure that paper and electronic health records are stored, transferred and disposed of in a secure manner. Follow College guidelines for retention periods.

Step 9: Vendor Contracts

You should look at your contracts with your vendors (especially your electronic health record provider, software vendors, back up, IT services, 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 clients.

Step 10: Conduct a Privacy Inventory and Audit

You should inventory the personal health information you hold and 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 practice and assigned deadlines. You also must audit activity of any staff who use your electronic health records.

Step 11: Interoperability Standards

Any time you change or update your information systems (including your electronic health record or software relating to health records) you must ensure all your digital assets comply with Ontario Health's interoperability standards.

Step 12: 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. There are certain types of breaches that must be reported to the Commissioner right away. Follow the Commissioner's guidelines on responding to a health privacy breach.

Step 13: Report your privacy statistics and trends

You have mandatory annual tracking and reporting of privacy breaches to the IPC. You may also 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.

Step 14: 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 clients, damages to clients, equipment impact and other risks.

Privacy Officer Supports

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

Health Privacy Officer Foundations training – next course starts Fall 2023

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