The College of Naturopaths of Ontario

Regulatory Guidance

Navigating PHIPA: Best Practices for Recordkeeping

In Ontario, those who collect and retain personal health information (PHI) are referred to **Health Information Custodians** (custodians) under *the Personal Health Information Protection Act, 2004* (PHIPA). Custodians have several obligations related to the collection, use, and disclosure of PHI designed to protect patient privacy. In most cases, the naturopathic doctor is the custodian of their patients' records, meaning that they are the ones who have custody and control of them and are responsible for securing and maintaining the records in accordance with PHIPA. However in certain circumstances, for example, when a registrant is practising as a locum or is retained by a multidisciplinary clinic, another health care provider or the clinic owner may be designated as the custodian. The patient must always be aware of who has custody and control of their personal health information and how their information will be managed.

The custodian is ultimately accountable for ensuring that their patients' PHI is collected, used, and disclosed in ways that safeguard their rights and privacy. This accountability applies not just during the active life of a patient file, but until that information is securely destroyed or legally transferred to a successor who becomes the new custodian.

The Information and Privacy Commissioner of Ontario (IPC) provides several resources to help health care practitioners in Ontario comply with the privacy requirements set out in PHIPA. Some information for NDs to consider is laid out below. Additionally, at the end of this article you will find a **Privacy Practices Template** that you can post within your clinic with important information for your patients.

Governance and Accountability

The importance of privacy should be one of the central considerations for any health care provider who collects PHI. Some important things to consider are:

- **Appointing a Privacy Officer:** Regardless of the size of the practice, you need to designate a privacy officer (which may be yourself) to oversee the daily implementation of privacy policies. This role involves identifying risks to patient privacy, handling patient inquiries, and managing any potential breaches. A breach occurs when PHI is unintentionally disclosed to an unauthorized party.
- **PHI Inventory:** The Privacy Officer should be aware of the PHI you hold, where and how it is stored, and how long it must be retained.

- **Vetting Service Providers:** Many NDs rely on third-party companies for things like Electronic Medical Records (EMR) or billing. Remember that you remain accountable for the privacy of the data handled by these providers, and you need to ensure that they are compliant with PHIPA.

Safeguarding Personal Health Information

PHIPA requires NDs to take "reasonable steps" to protect PHI against theft, loss, and unauthorized access. Elements of this include:

- **Technical Safeguards** such as **encryption, access controls** to ensure that only those who need the information to perform their duties have access, and **logging information** that records those who access or modify PHI.
- **Physical and Administrative Safeguards** such as a **secure environment** and **appropriate training** for staff and other providers who may be present or have access to PHI. You may consider implementing annual confidentiality agreements that outline the importance of compliance.

Privacy Breaches

A privacy breach occurs if PHI is lost, stolen, or shared without authorization. If a breach occurs, you should try to determine the scope of the breach and what information was disclosed. Do your best to retrieve the information and stop further unauthorized access.

You will need to notify those affected by the breach directly and as soon as possible. You can do this by phone, email, letter, or in person. Under PHIPA, custodians must also report certain privacy breaches to the IPC at the first reasonable opportunity. The circumstances that determine if you are required to report the breach to the IPC are set out in PHIPA. More information on when to report to the IPC can be found here.

If the breach involves a member of a regulated health profession, you may also be required to notify their regulatory college about the breach. This should be done within 30 days if any of the following applies:

- You terminate or suspend the individual because of the breach, or you restrict their privileges or access to PHI.
- The individual resigns from their position at your clinic or voluntarily restricts their privileges or access to PHI and you believe this is done because of the breach.

You are not required to notify this College because of a breach. You should follow the directions as outlined above to contain the breach and be sure to carefully document this in the patient records of those affected. You should also take steps to ensure such a breach does not occur again by examining your privacy policies and protocols and implementing changes as needed.

Record Retention and Succession Planning for PHI

A change in practice can occur due to planned events like retirement or relocation but can also happen unexpectedly due to unforeseen circumstances such as sudden illness. You should have a clear plan in place for what happens to your patients' PHI if you retire, move, or are prevented from continuing to practice unexpectedly. Succession planning helps to ensure that you protect your patients from an interruption to their health care or a breach of their privacy because of these changes. It can also make a practice transition much smoother by avoiding any disputes with clinic owners over who retains patient records when leaving a clinic.

Remember, your obligations as a custodian under PHIPA do not end until a legally authorized successor assumes accountability for any records that are in your custody (or until records are securely destroyed after retention periods expire). NDs are required to maintain and retain records for a period of at least 10 years after the date of the last entry. In the case of a minor, records are retained for at least 10 years following the patient's 18th birthday, regardless of the date of the last entry.

Key Components of a Succession Plan

To be effective, your succession plan must identify the new custodian (if applicable) and detail exactly how records will be managed when you move locations or stop pratising.

Key considerations include:

Identification of the Successor Custodian

The plan must clearly name who will take over the records (or if they will be remaining with you as a custodian at a new practice location). Larger or multidisciplinary clinics should have agreements in place that specify what happens to the PHI of each practitioner's patients during a change in practice.

- **Transfer:** You may transfer records to a successor who is currently a custodian or who will become one (e.g., a new naturopathic doctor taking over your practice when you retire).
- **Retention:** You retain the only copy of the records when you move locations.
- **Copy: A copy of a patient record cannot be made without the written consent of the patient first**. In this case, the person being provided with a copy of the record also becomes a custodian.
- **In Case of Death:** If you pass away, your estate trustee or the person administering your estate automatically becomes the custodian until the records are passed to another authorized person.

Responsibilities During the Transition

The plan must specify who is responsible for the following important tasks:

- **Secure Storage:** Ensuring records continue to be stored appropriately.
- **Access:** Managing patient requests for copies or updates to their health information.
- **Secure Copying, Transfer or Disposal:** Overseeing the encrypted copying or transfer of digital files or their permanent destruction once retention periods expire.
- **Managing Third Party Companies:** Ensuring any third party companies involved during a transition (for example, a records storage company) abide by privacy practices on your behalf.

Notification Obligations

Your plan must include a protocol for notifying patients about any change in practice location or custodian and what will happen with their PHI.

- **Timing:** Patients must be given reasonable notice before a change in practice location occurs. If their PHI is being copied, their consent must be obtained beforehand. They should also be notified before their PHI is transferred to a successor custodian or, if that isn't feasible, as soon as possible afterward.
- **Method:** Direct notification (letter, email, phone call, or in-person) is preferred. If contact information is out-of-date, indirect notice (website or social media posts) can be used.
- **Content:** The notice must describe the practice change that will take place, provide contact information if a new custodian will be retaining their PHI, state how long records will be kept, and explain how they can request a transfer to a different custodian if they would prefer this option.

Regardless of whether you are moving or closing your practice, the College must also be notified.

- **Moving Locations:** You will need to update your practice location in your College profile within 14 days of a change of address.
- **Closing or Selling Your Practice:** When PHI is transferred to a new custodian, then the College must be made aware of this in writing. You will need to provide the College with the address of where records will be stored for a minimum of 10 years from the date of your last day of practice.

Additional Resources

PHIPA, 2004
A Privacy Management Handbook for Small Health Care Organizations
Standard of Practice for Record Keeping
Website of the Information and Privacy Commissioner of Ontario
Regulatory Guidance: Transfer of Records
Regulatory Guidance: Obligations When Changing or Closing a Practice Location

Appendix A: Privacy Practices Template

Appendix A: Privacy Practices Template

Below is a template designed to meet the transparency requirements for a naturopathic clinic in Ontario under PHIPA. Registrants can customize the bracketed information to reflect their specific practice details.

Public Statement on Privacy Practices

[Name of Clinic]

At **[Name of Clinic]**, we are committed to protecting the privacy of our patients and ensuring the confidentiality of the personal health information (PHI) entrusted to us. This statement summarizes our policies and your rights regarding your health records.

Commitment to Your Privacy

As **Health Information Custodians (HICs)** under the *Personal Health Information Protection Act, 2004* (PHIPA), we have a legal duty to protect your records from loss, theft, and unauthorized access, use, or disclosure.

Collection and Use of Your Information

We collect your personal health information—including your health history, laboratory results, and treatment recommendations—primarily to provide you with quality naturopathic care. We may also use this information for:

- **Billing and Payment:** To process claims with private insurers or for internal accounting.
- **Quality Improvement:** To review our clinical practices and ensure we are meeting professional standards.
- **Legal Requirements:** To comply with mandatory reporting to regulatory bodies or as otherwise required by law.

Sharing Your Information (Disclosure)

We will obtain your **express written or verbal consent and document it in your health record** before sharing your information with third parties, such as:

- Other health care providers
- Insurance companies
- Legal representatives

Your Rights: Access and Correction

You have the right to view and receive a copy of your health records, including all laboratory results, at any time.

- **Requests:** To request access, please contact our Privacy Officer in writing (see below). We will respond as soon as possible, but within 30 days.
- **Fees:** We may charge a reasonable cost-recovery fee for preparing and sending your records.
- **Corrections:** If you believe your record is inaccurate or incomplete, you may request a correction.

Safeguards and Retention

We maintain your original records in a secure manner for at least **10 years** following your last visit (or 10 years after a minor's 18th birthday). Our safeguards include:

- Locked filing cabinets and restricted office access
- Encrypted digital storage
- Confidentiality agreements signed by all clinic staff

Contact Our Privacy Officer

If you have questions, concerns, or wish to make a formal complaint about our privacy practices, please contact:

[Name of Privacy Officer / Registrant]

[Clinic Address]

[Phone Number]

[Email Address]

You also have the right to complain to the **Information and Privacy Commissioner of Ontario** at 1-800-387-0073 or via www.ipc.on.ca .