PRIVACY FOR ONTARIO PHYSICIANS AND STAFF

OntarioMD
Empowered Practices. Enhanced Care.

Frequently Asked Questions

The following Frequently Asked Questions are intended to help physicians understand their legal and professional obligations to maintain the privacy of patients and the confidentiality of their personal health information under the Personal Health Information Protection Act, 2004 (PHIPA).

They are not meant to be construed as legal advice, nor do they address all matters pertaining to privacy and the confidentiality of personal health information.

Physicians should seek advice from the College of Physicians and Surgeons of Ontario (CPSO), the Canadian Medical Protective Association (CMPA), their legal counsel, or the Information and Privacy Commissioner of Ontario if they are uncertain about how to interpret the legal requirements of PHIPA.

Q1: What is PHIPA?

A1: The Personal Health Information Protection Act, 2004 (PHIPA) is the health-specific privacy legislation in Ontario. PHIPA governs the manner in which personal health information (PHI) may be collected, used and disclosed within the health care system, as well as its secure retention, transfer and disposal. The legislation also regulates individuals and organizations that receive PHI from health care providers. It further provides individuals with a right to access their records of PHI and to request that corrections or amendments be made.

Please review the resources section above for more information.

Q2: What is Personal Health Information (PHI)?

A2: Personal health information, or PHI, is "identifying information" collected about an individual, whether oral or recorded. It includes information about an individual's health or health care history in relation to:

- The individual's physical or mental condition, including family medical history;
- The provision of health care to the individual;
- Long-term care services;
- The individual's health card number;
- Blood, bodily substances or body-part donations;
- Payment or eligibility for health care; and
- The identity of a health care provider or a substitute decision-maker for the individual.

"Identifying information" includes health information that could identify an individual when used alone or in conjunction with other information.

Q3: What is a Health Information Custodian (HIC)?

A3: A HIC is a listed individual or organization under PHIPA that, as a result of his or its power or duties, has custody or control of PHI.

Examples of HICs include:

- Health care practitioners, (including doctors, nurses, audiologists and speech-language pathologists, chiropractors, chiropodists, dental professionals, dieticians, medical radiation technologists, medical laboratory technologists, massage therapists, midwives, optometrists, occupational therapists, opticians, pharmacists, physiotherapists, psychologists and respiratory therapists);

Q4: What is the role and what are the responsibilities of a HIC?

A4: PHIPA requires HICs who have custody or control of PHI to establish and implement information practices that comply with its provisions. This does not mean that custodians are expected to completely set aside their existing policies and practices. In fact, PHIPA builds upon existing policies and guidelines for health care:professionals and provides enforceable rules relating to the collection, use or disclosure of PHI as well as its secure retention, transfer and disposal.

For example, PHIPA requires HICs to:

- Obtain an individual's consent when collecting, using and disclosing PHI, except in limited circumstances as specified under PHIPA;
- Only collect, use and disclose PHI were it is necessary and no more than is reasonably necessary;
- Take reasonable precautions to safeguard PHI, including:
  - Protection against theft or loss; and
  - Protection against unauthorized use, disclosure, copying, modification or destruction;
- Notify an individual at the first reasonable opportunity if PHI is stolen, lost or accessed by an unauthorized person;
- Ensure health records are as accurate, up-to-date and complete as necessary for the purposes which they use or disclose PHI;
- Ensure health records are retained, transferred and disposed of in a secure manner;
- Designate or take on the role of a contact person who is responsible for:
  - Responding to access/correction requests;
  - Responding to inquiries about the custodian's information practices;
  - Receiving complaints regarding any alleged breaches of PHIPA; and
  - Ensuring overall compliance with PHIPA.
- Provide a written statement that is readily available to the public and describes:
  - A custodian's information practices;
  - How to reach the contact person; and
  - How an individual may obtain access, request a correction or make a complaint regarding his/her PHI.
- Inform an individual of any uses and disclosures of PHI without the individual's consent that occurred outside the custodian's information practices; and
- Ensure that all agents of the custodian are appropriately informed of their duties under PHIPA.

Q5: What is an Electronic Service Provider?

A5: Under s. 10(4) of PHIPA, an electronic service provider is a person who provides goods or services for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain or dispose of PHI. Where an electronic service provider is not an agent of a HIC, under Ontario Reg. 329/04, s. 6(1) the electronic service provider must not use any PHI to which it has access in the course of providing the services for the HIC except as necessary in the course of providing the services, must not disclose any such PHI and must not permit its employees or any person acting on its behalf to access PHI unless the employee or person acting on its behalf agrees to comply with these restrictions. An electronic service provider may have PHI in its systems during the provision of a service, however the HIC remains fully accountable to the patient for protecting privacy and maintaining the confidentiality of the PHI.

Q6: What is a Health Information Network Provider (HINP)?

A6: A HINP is a special type of electronic service provider. Under Ontario Reg. 329/04, s. 6 (2), a HINP is defined as, "a person who provides services to two or more HICs where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose PHI to one another, whether or not the person is an agent of any of the custodians."

A HINP may have PHI in its systems during the provision of a service, however the HIC remains fully accountable to the patient for protecting privacy and maintaining the confidentiality of the PHI.

Q7: What is the role and what are the responsibilities of a HINP?

A7: In addition to the roles and responsibilities that apply to all electronic service providers under Ontario Reg. 329/04, s. 6(1), HINPs have additional roles and responsibilities under Ontario Reg. 329/04, s. 6(3). For example, HINPs must:

- Notify the custodian at the first reasonable opportunity of any breaches;
- Perform threat risk and privacy impact assessments;
- Provide an audit trail of all accesses and transfers of PHI held in equipment controlled by the HINP;
- Ensure that third parties retained by the HINP comply with the restrictions under Ontario Reg. 329/04, s. 6(3);
- Enter into a written agreement with the custodian that describes the services that the HINP is required to provide, the safeguards in relation to the confidentiality and security of the PHI and requires the HINP to comply with PHIPA and its regulations; and
- Make publicly available information about the HINP's services to the custodian.

Q8: What is a privacy breach?

A8: A privacy breach occurs whenever a person has contravened or is about to contravene a provision of PHIPA or its regulations, including section 12(1) of PHIPA.

A privacy breach includes the collection, use or disclosure of PHI that is not in compliance with applicable privacy law, and circumstances where PHI is stolen, lost or subject to unauthorized use, disclosure, copying, modification, retention or disposal.

Q9: What should you do in the event of a privacy breach?

A9: Upon learning of a privacy breach, immediate action must be taken. The Information and Privacy Commissioner of Ontario (IPC) advises HICs to follow the following steps simultaneously or in quick succession in the event of a privacy breach:

Step 1: Respond immediately by implementing the privacy breach protocol

- Ensure appropriate staff within your organization are immediately notified of the breach, including the Chief Privacy Officer or contact person for the purposes of PHIPA;
- Depending on the nature or seriousness of the privacy breach, there may be a need to contact senior management, patient relations or the information and technology and/or communications department within your organization;
- Consider informing the IPC Registrar of the privacy breach and work together constructively with IPC staff; and
- Address the priorities of containment and notification as set out in the following steps.

Step 2: Containment - Identify the scope of the potential breach and take steps to contain it

- Retrieve the hard copies of any PHI that has been disclosed;
- Ensure that no copies of the PHI have been made or retained by the individual who was not authorized to receive the information and obtain the person's contact information in the event that follow-up is required; and
- Determine whether the privacy breach would allow unauthorized access to any other PHI (e.g. an electronic information system) and take whatever necessary steps are appropriate (e.g. change passwords, identification numbers and/or temporarily shut down a system).

Step 3: Notification - Identify those individuals whose privacy was breached and notify them of the breach

- PHIPA requires HICs to notify individuals, at the first reasonable opportunity, but does not specify the manner in which notification must be carried out;
- For example, notification can be by telephone or in writing, or depending on the circumstances, a notation made in the individual's file to be discussed at his/her next appointment;
- There are numerous factors that may need to be taken into consideration when deciding on the best form of notification (e.g. the sensitivity of the PHI). As a result, the HIC may want to contact the IPC to discuss the most appropriate form of notification;
- There may also be exceptional circumstances when the HIC may want to discuss notification with the IPC before proceeding (e.g. when direct notification is not possible or may be detrimental to the individual). If this is the case, the HIC is encouraged to contact the IPC to discuss these circumstances;
- When notifying individuals affected by the breach, provide details of the extent of the breach and the specifics of the PHI at issue;
- Advise affected individuals of the steps that have been or will be taken to address the breach, both immediate and long-term; and
- Advise that the IPC has been contacted to ensure that all obligations under PHIPA are fulfilled (where applicable).

Step 4: Investigation and Remediation

- Conduct an internal investigation into the matter. The objectives of the investigation are to: 1) ensure the immediate requirements of containment and notification have been addressed; 2) review the circumstances surrounding the breach; and 3) review the adequacy of existing policies and procedures in protecting PHI;
- Address the situation on a systemic basis. In some cases, program-wide procedures may warrant review (e.g. a misdirected fax transmission);
- Advise the IPC of your findings and work together to make any necessary changes;
- Ensure staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of PHIPA; and
- Cooperate in any further investigation into the incident undertaken by the IPC.

Q10: Where can I get help on privacy and security considerations within my practice?

A10: OntarioMD offers support to physicians on privacy and security considerations for their practices, including obligations under PHIPA when undergoing an EMR migration.
Please visit https://www.ontariomd.ca/idc/groups/public/documents/omd_file_content_item/omd011945.pdf to download the Privacy and Security Guide, consult with your OntarioMD Practice Management Consultant or contact OntarioMD at info@ontariomd.com.

Additional Sources:

- "Confidentiality of Personal Health Information" - The College of Physicians and Surgeons of Ontario: http://www.cpso.on.ca/policies-publications/policy/confidentiality-of-personal-health-information

- "Frequently Asked Questions, Personal Health Information Protection Act, February 2005"
- Information and Privacy Commissioner/Ontario: Ann Cavoukian, Ph.D, Commissioner
- https://www.ipc.on.ca/images/Resources/hfaq-e.pdf

- "What to do When Faced With a Privacy Breach: Guidelines for the Health Sector"
- Information and Privacy
Commissioner of Ontario - https://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf

OntarioMD
Empowered Practices. Enhanced Care.