Electronic Medical Records – Transition Support Program

Privacy and Security Guide and Workbook

Version 1.2

OntarioMD

About this Document

The purpose of the Privacy and Security Guide and Workbook for Electronic Medical Records (EMRs) is to provide relevant information, tools and considerations regarding privacy and security to support practices that are planning, implementing and/or using EMRs. It is intended to be complementary to physicians' existing professional responsibilities to their patients and shifts the focus on the practice considerations related to health information privacy in the use of EMRs.

Although the wording throughout this document is such that it is addressed to physicians (including specialists), it applies to a broader audience within the primary care practice setting. It should be read and followed by the practice lead as well as the practice's designated privacy contact.

It addresses both general privacy and security considerations, as well as additional considerations related to EMRs. These are addressed in Part 1 and Part 2 of this document, respectively.

Central to this document is the assessment of your practice's privacy and security requirements, and the identification of many resources and tools to support a practice in better understanding and meeting privacy and security requirements as required.

It is the responsibility of the practice to ensure that all its employees and third parties comply with privacy and security requirements. OntarioMD Practice Management Consultants and Peer Leaders can assist in understanding and planning to address these requirements.

Note: OntarioMD does not purport to be the authoritative source of privacy legislation or policies. It has developed the Privacy and Security Guide and Workbook for EMRs in line with its role in providing assistance and guidance to physicians and their staff. This document should not replace the practice's own review and understanding of legislation and/or advisement of legal counsel.

Table of Contents

Introduction

Ontario's Personal Health Information Protection Act (PHIPA) was introduced in 2004. PHIPA pertains to the collection, use and disclosure of Personal Health Information (PHI) by organizations and individuals delivering health care. This legislation sets out a number of responsibilities and requirements for health care providers in the delivery of care in Ontario, and in particular the responsibilities of Health Information Custodians (HICs) – whether managing and storing patient records in a paper-based or electronic practice environment. Importantly PHIPA provides patients with a right to request access to, and correction of, their health records.

Key Concepts

This section provides high level descriptions of some key concepts regarding privacy and security. Please refer to the Additional Resources provided at the end of this document for more information.

Privacy and Security

Although the terms privacy and security are related and often used together, they are two distinct concepts that need to be considered separately to ensure the protection of patients' personal health information.

- **Privacy** addresses who is authorized to access patient information and under what circumstances this information may be accessed, used, or disclosed to third parties authorized to receive it. Privacy is often addressed through the implementation of rigorous policies and procedures.
- **Security** controls access and protects information from accidental or intentional disclosures to unauthorized persons. Different types of technology, physical safeguards and processes can be used to address security.

This section presents an overview of core concepts pertaining to privacy and security in a health care environment. These include: personal health information, health information custodians, and various patient considerations.

Personal Health Information

PHI is any identifying information about an individual in oral or recorded form, if it:

Personal Health Information (PHI)
is any identifying information about an individual, and could relate to any of: physical or mental health, family health history, health care provided, eligibility for health care services, health number, and substitute decision maker.

- Relates to the physical or mental health of the individual (including health history of the individual's family)
- Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- Is a plan of service within the meaning of the Home Care and Community Services Act, 1994 for the individual,

- Relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
- Relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
- Is the individuals' health number, or
- Identifies an individual's substitute decision-maker

Health Information Custodians

PHIPA both defines and specifies requirements for those individuals who are considered to be health information custodians (HICs). A HIC has custody or control of personal health information as a result of their job responsibilities.

Health Information Custodians include doctors, health care practitioners, hospitals, long-term care facilities, health care clinics, laboratories, pharmacies, the Ontario Ministry of Health and Long-term care and other health-related organizations.

PHIPA also defines the role of an agent who is a person who acts for, or on behalf of the HIC in respect of personal health information for the purposes of the custodian. Agents may include a wide range of individuals who exercise different roles where some agents have access to the complete records of personal health information and others only a part. Examples include employees of the HIC, information technology service providers, and providers of records management services or claims management services. HICs may permit agents to collect, use, disclose, retain or dispose of personal health information as they hold decision making power for PHI in their custody or control. Agents also have clear obligations set out in the regulations under PHIPA.

A further defined group under PHIPA is a Health Information Network Provider (HINP) who is a person who provides services to two or more HICs where the service is primarily provided to enable HICs to use electronic means to disclose PHI to one another. PHIPA imposes additional obligations on HINPs to notify HICs of unauthorized accesses to PHI, to provide service and policy information, maintain audit trails, along with assessments of their services to ensure the security and integrity of PHI is maintained. Vendors of EMRs will have additional obligations if they meet the definition of an HINP.

When a HIC becomes aware of a privacy breach they are required to take immediate action to respond, contain, notify, investigate and remediate the breach as appropriate. See the Additional Resources section for a helpful guide provided by the Office of the Information and Privacy Commissioner of Ontario on this topic.

Patient Considerations

Patients have a right to access their PHI and to obtain a copy of it upon request. They may also request corrections to their PHI if they believe that their record is inaccurate or incomplete; requests should be made in writing to the HIC and should contain sufficient detail to enable the HIC to identify and locate the record with reasonable efforts. The HIC may charge patients a fee for copies of their PHI if they first provide an estimate of the fee; the HIC may also waive

this fee. The Ontario Medical Association updates its Physician's Guide to Third Party and Other Uninsured Services on an annual basis; it contains advice on the appropriate amount to charge patients for copies of their PHI. It can be accessed online by OMA members here: https://www.oma.org/Member/Resources/Documents/ThirdPartyGuide.pdf.

HICs are required to respond as soon as possible but no later than 30 days after receiving the request. If the HIC requires justifiable additional time to respond to the request, the HIC should provide to the patient written notice of the extension as well as the reason for the extension. PHIPA also indicates that a HIC may refuse to grant a patient the requested information or correct the patient's request for a correction if they believe that the reason for access is "frivolous or vexatious or is made in bad faith".

In two types of circumstances, HICs are not permitted to assume consent but must obtain express consent from an individual. This is required when a HIC discloses a patient's PHI to someone who is not a HIC (such as an insurer or family member), or when a HIC discloses PHI to another HIC for a purpose other than providing (or assisting in providing) health care.

HICs should be prepared to address any inquiries or complaints related to privacy and security, maintaining proper documentation to support its actions and practices. HICs must also make available a public statement regarding information practices.

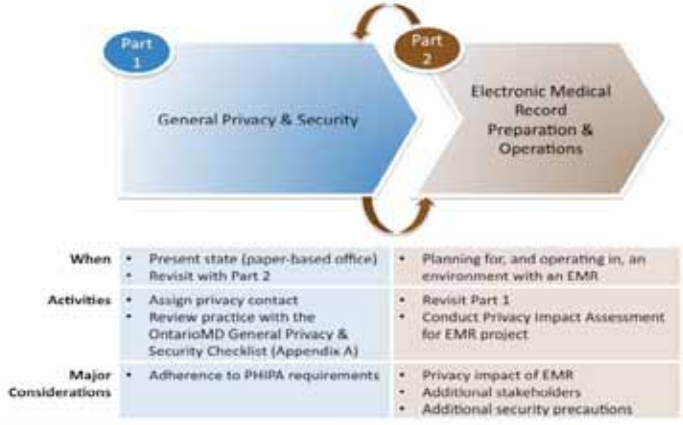
Overview of Parts 1 and 2

This document addresses both 1) general privacy and security considerations, as well as 2) additional considerations to be made in preparation for (and in operating in an environment using) an EMR. These are addressed in Part 1 and Part 2 of this document, respectively.

Part 1 can and should be undertaken at any time (even if there is not yet an EMR in place), if PHIPA requirements have not yet been addressed by a practice or if it is believed that another review and improvement on a practice's PHIPA adherence is required. Part 2 should be undertaken when planning for an EMR (or even if one is in place and there is the need to review the current practices and environment).

This framework is presented in the figure below. Parts 1 and 2 are described in more detail in the subsequent sections of this document.

Privacy & Security Guide and Workbook Framework



Part 1: General Privacy & Security

Objectives

To re-visit and understand a practice's basic obligations regarding PHIPA compliance, in either a paper- or electronic-based environment.

Overview

Whether in a paper-based or electronic environment, healthcare providers continue to have a duty to ensure that personal health information within their custody is protected at all times.

Privacy is the law. In Ontario it is enforced by the Office of the Information Privacy Commissioner (IPC), which can apply, and has applied, PHIPA provisions in health care environments. To comply with PHIPA, a practice must adhere to a number of requirements around the collection, use and disclosure of PHI.

Additionally, practices should make provisions for security measures including physical safeguards of office space and equipment (during and after hours of operation). Further, technical security measures and policies pertaining to password protection and management, data encryption, and secure connections should be addressed.

Activities

One of the first steps for a practice to take, which itself is a requirement of PHIPA, is to assign a privacy contact, if one has not already been designated. This person will play a key role in coordinating and conducting privacy and security activities – initially and on an ongoing basis.

The General Privacy & Security Checklist (provided in Appendix A) presents the basic privacy and security considerations that a practice needs to have in place to comply with PHIPA. It also presents helpful resources (including information and templates) to assist

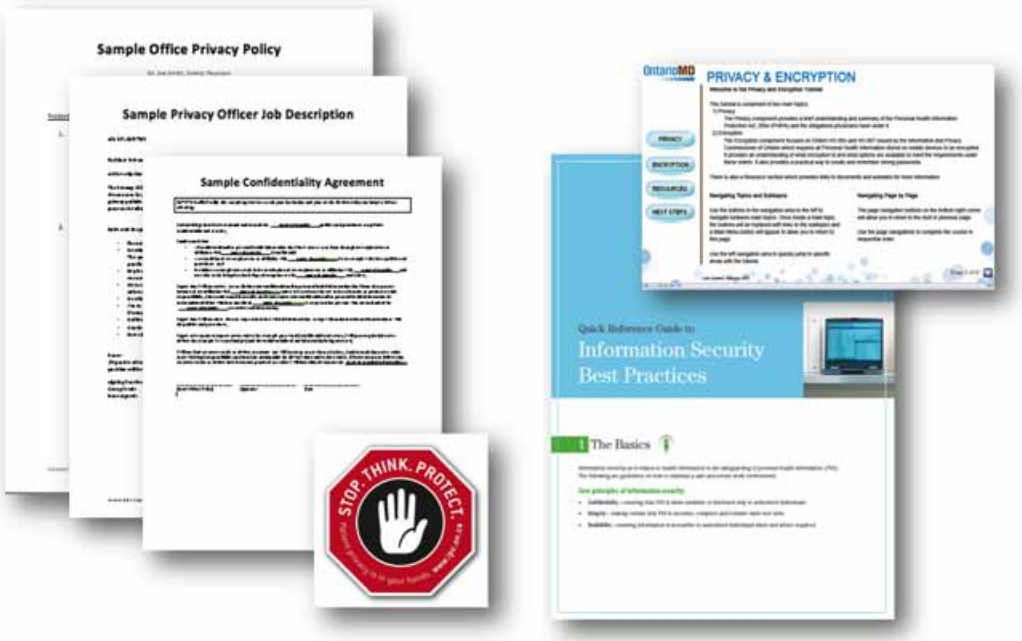
To comply with PHIPA, practices must:

1. Designate a privacy contact person,
2. Identify the purposes for collection, use and disclosure personal health information,
3. Only collect, use and disclose patients' personal health information if they have their consent to do so or if the Act allows them to do so without consent,
4. Only collect, use and disclose patients' personal health information if no other information would serve the purpose,
5. Only collect, use and disclose that amount of information necessary to serve the purpose,
6. Take reasonable steps to ensure that patients' personal health information is as accurate, complete and up-to-date as needed for its use or disclosure,
7. Establish and maintain appropriate information practices and tell patients about these practices,
8. Develop and make available a written statement,
9. Develop procedures to identify inappropriate use or disclosure of PHI, notify affected patients, and make and keep notes of such a use or disclosure in or linked to the affected patient's personal health record,
10. Train staff, volunteers and others acting on their behalf, and
11. Take reasonable steps to protect personal health information that they transfer to others (for example, including privacy clauses in contracts. with agents).

practices to better meet and enhance adherence to these privacy and security requirements. Section 7 of the checklist specifically addresses security and refers to a Quick Reference Guide to Information Security Best Practices developed by eHealth Ontario to address matters such as: password security, backups, email practices, mobile computing and hardware protection, and security incidents. It provides considerations for the places where PHI can be found throughout and beyond the practice to guide physicians in protecting all information, in various forms. Another key resource is the OntarioMD Privacy & Encryption Tutorial (https://www.ontariomd.ca/idc/groups/public/documents/omd_file_content_item/omd011555.swf).

In addition, or alternatively, a practice may choose to assess its privacy and security practices using the Canadian Medical Association's (CMA) Privacy Wizard and Practice Management Diagnosis Tool (www.cma.ca/tools), which is available online to CMA members only. Upon completing this activity, a number of customized outputs are generated for use. These include a privacy statement handout for patients, a detailed record of office privacy policies, practices and procedures, a list of suggested privacy enhancements for an office, and sample forms and clauses. These can also be provided as generic templates by OntarioMD representatives, and are referenced in Appendix A.

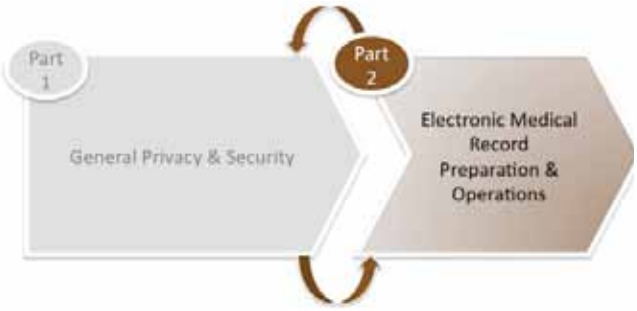
Sample Resources and Tools



Part 2: EMR Preparation & Operations

Objectives

To address additional privacy and security considerations in preparation for, and in operating in, an environment associated with an Electronic Medical Record (EMR).



Overview

As a practice begins to plan and implement an EMR, it is an opportune time to re-visit privacy and security requirements. In some cases this may involve reviewing current privacy and security measures, and enhancing them as applicable for an electronic information environment. In other cases, there will be new privacy and security requirements to meet as they are specific to the use and operation of a new EMR.

Note that there also are privacy and security considerations to analyze and address in planning and implementing the Electronic Medical Record. Although these are not necessarily directly required by law, many are interim steps to assist in planning and preparing for ongoing compliance and best practice with respect to privacy and security (for example, some of the activities lead to the development of artifacts that are required by law).

There are a number of Privacy and Security Guidelines detailed in the Vendor and Physician Checklist, which is an addendum to the Physician and Vendor contract (Appendix A). The EMR Vendor will be contractually obligated to address or facilitate some of these privacy and security requirements for a practice. Practices should ensure that they discuss the obligations of partnering with potential EMR vendors moving forward.

Activities

A two-step approach (not necessarily in chronological order) is recommended, as follows:

1. Re-visit Part 1 of this document (General Privacy & Security). Ensure that policies and practices reflect the impending or new EMR-associated environment. These could arise from changes in stakeholders (such as additional or different IT service providers) and changes to a practice's use of PHI.

2. Conduct a Privacy Impact Assessment (PIA) for the EMR project. Guidelines for conducting a Privacy Impact Assessment (PIA) have been developed by the Information and Privacy Commissioner of Ontario. The Guideline a self assessment tool to assist HICs in reviewing the impact that a system, technology or program may have on the privacy of an individual's personal health information under PHIPA.

Note that a PIA is specific to a particular technology, and that this assessment should be conducted even if a practice is moving from one EMR system to another.

These PIA Guidelines can be found online, here: http://www.ipc.on.ca/images/Resources/up-phipa_pia_e.pdf.

Again - in addition, or alternatively, a practice can use the Canadian Medical Association's (CMA) Privacy Wizard and Practice Management Diagnosis Tool (www.cma.ca/tools), which is available online to CMA members only.

Appendix A: General Privacy & Security Checklist

Provisions	Evaluation			Information and Tools for Enhancement		
	Yes	Somewhat	No	Useful tools	Description	Comments and Additional Considerations
Privacy Contact Person						
1. Privacy contact person for the practice has been identified.	☐	☐	☐	Security Officer Responsibilities – within the Guide to Information Security for the Health Care Sector: Information and Resources for Small Medical Offices. (http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_SmallOffices.pdf)	This resource provides 14 responsibilities of a security officer for the practice, to incorporate into job descriptions, policies and processes. (Source: eHealth Ontario)	• The privacy contact person should be a physician. • Designate backup/ contingency contact as well. • The privacy contact may also be the security officer; in some cases a separate technical lead may address security.
2. Privacy contact person is adequately and sufficiently educated and trained.				Personal Health Information Protection Act, 2004 (http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm)	This is the full, electronic version of Personal Health Information Protection Act, 2004.	• Ensure backup/ contingency contact is also educated and trained. • Ensure that adequate and sufficient documentation is developed and maintained. • Examples of responsibilities of the contact person(s) include: * Monitoring of compliances and breaches to policies; escalation as required and notification to patients * Ensuring ongoing understanding and agreements of staff and third parties * Communication and dissemination of policies and information
				A Guide to the Personal Health Information Protection Act (http://www.ipc.on.ca/images/resources/hguide-e.pdf)	Although not an official legal interpretation of the legislation, this is a shorter and practical guide to PHIPA. (Source: Information Privacy Commissioner/Ontario)	
				OntarioMD Privacy & Encryption Tutorial (https://www.ontariomd.ca/idc/groups/public/documents/omd_file_content_item/omd011555.swf)	This is an online tutorial developed by OntarioMD that provides an overview of privacy and encryption.	
				Guide to Information Security for the Health Care Sector: Information and Resources for Small Medical Offices. (http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_SmallOffices.pdf)	This is a resource provided by eHealth Ontario for small medical offices such as physician offices and family health teams. It provides a framework for applying security controls for the protection of personal and personal health information. Responsibilities are outlined for the following stakeholders: security officer, staff, and IT service provider. (Source: eHealth Ontario)	
				Commissioner Cavoukian Blog (http://blogs.itbusiness.ca/2010/10/a-challenge-to-health-it-professionals-patient-privacy-is-in-your-hands/)	A practice's privacy contact can follow Ontario's Information & Privacy Commissioner for information and updates.	

Appendix A: General Privacy & Security Checklist

Provisions	Evaluation			Information and Tools for Enhancement		
	Yes	Somewhat	No	Useful tools	Description	Comments and Additional Considerations
Policies and Practices						
3. Existence of a written privacy policy addressing the collection, use, disclosure and retention of PHI in accordance with PHIPA and other applicable legislation.	☐	☐	☐	Sample Office Privacy Policy (Click here to access the template provided)	This is a sample privacy policy from which a practice can copy the text and customize content to reflect office information practices. (Source: Canadian Medical Association)	• Also ensure compliance - that policies are actually implemented, followed and monitored. • Establish and follow practices for identifying and addressing suspected and actual privacy breaches.
				Sample Security Policy – within the Guide to Information Security for the Health Care Sector: Information and Resources for Small Medical Offices. (http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_SmallOffices.pdf)	This is a sample security policy that can be used by a practice to document and reflect a practice's adherence to legal obligations with respect to PHIPA. (Source: eHealth Ontario)	
4. Existence of a written public policy regarding the practice's information practices, who to contact with privacy questions or complaints, and how to obtain access or request correction of a record of personal health information.	☐	☐	☐	Sample Privacy Policy (Click here to access the template provided)	This is a sample privacy policy, addressed to patients, for use in physicians' offices. (Source: Ontario Medical Association)	• Public policies should be readily accessible to patients. This could occur in any number of ways (e.g., a paper copy could be on-hand to be shown to anyone who requests it, an electronic copy could be made available and/or posted on the practice's website, a printed copy could be posted in the practice). • Ensure that a practice is prepared by having necessary consent management practices and policies in place.
				Sample Office Privacy Handout. (Click here to access the template provided)	This is a sample handout for patients regarding a office's privacy practices. (Source: Ontario Medical Association)	
				General Privacy Statement (handout) for Patients (Click here to access the template provided)	This is a sample statement of a physician office's information practices. It is available in English and French. (Source: Canadian Medical Association)	
				Your Health Information and Your Privacy In Our Office – brochure (http://www.ipc.on.ca/images/Resources/up-BrochOffice.pdf)	This brochure describes privacy practices and informs patients on how to exercise their rights under PHIPA. Also available in printed format (contact the IPC/Ontario). (Source: Information Privacy Commissioner/Ontario)	
				Health Information Privacy In Our Office – poster (http://www.ipc.on.ca/images/Resources/up-PosterOffice.pdf)	This poster provides basic information to patients about PHI and privacy.. It refers patients to the brochure above, as well as the practice's privacy statement. Also available in printed format (contact the IPC/Ontario). (Source: Information Privacy Commissioner/Ontario)	

Appendix A: General Privacy & Security Checklist

Provisions	Evaluation			Information and Tools for Enhancement		
	Yes	Somewhat	No	Useful tools	Description	Comments and Additional Considerations
Understanding and Agreements						
5. Staff understand, agree to, and comply with privacy and security requirements.	☐	☐	☐	Confidentiality Agreement for Physician Office Employees (Click here to access the template provided)	This is a sample confidentiality agreement that a practice's employees can sign to reflect their understanding and compliance to office information practices. (Source: Canadian Medical Association)	• Ensure that employees understand the concepts reflected in the agreement. Provide information, educational tools and/or sessions as necessary.
				Confidentiality Agreement – Sample (Click here to access the template provided)	This is a sample confidentiality agreement for physician office staff. (Source: Ontario Medical Association).	
				Sample Contractual Privacy Clause for Employees and Third Parties. (Click here to acess the template provided)	This is a sample confidentiality clause that can be used to add to existing agreements with employees or third parties. (Source: Canadian Medical Association)	
				Staff Security Responsibilities – within the Guide to Information Security for the Health Care Sector: Information and Resources for Small Medical Offices. (http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_SmallOffices.pdf)	This resource provides 11 security responsibilities of staff in a practice, to incorporate into job descriptions, policies and processes. (Source: eHealth Ontario)	
				Article for health care providers. (http://www.ipc.on.ca/site_documents/stop_think_protect.pdf)	This is a 2 page article for health care providers on the use of PHI (particularly in mobile contexts). This can be incorporated into newsletters or other practice materials. (Source: Information Privacy Commissioner/Ontario)	
				Stop.Think.Protect Stickers. Send an email to info@ipc.on.ca to order some. Download in high resolution here: http://www.ipc.on.ca/site_images/STP_logo_hr.jpg	These stickers can be placed in various places around a practice. Logos can be used in newsletters, web pages and more. (Source: Information Privacy Commissioner/Ontario)	

Appendix A: General Privacy & Security Checklist

Provisions	Evaluation			Information and Tools for Enhancement		
	Yes	Somewhat	No	Useful tools	Description	Comments and Additional Considerations
6. Third parties understand, agree to, and comply with privacy and security requirements.	☐	☐	☐	Confidentiality Agreement for Third Parties. (Click here to access the template provided)	This is a sample confidentiality agreement that a practice's third parties (such as other health providers, researchers) can sign to reflect their understanding and compliance to office information practices. (Source: Canadian Medical Association)	• IT service providers could be many, and may include: * Help desk and/or technical support * Network providers * Providers of hosting services * EMR vendor
				Sample Contractual Privacy Clause for Employees and Third Parties. (Click here to access the template provided)	This is a sample confidentiality clause that can be used to add to existing agreements with employees or third parties. (Source: Canadian Medical Association)	
				IT Service Provider Responsibilities – within the Guide to Information Security for the Health Care Sector: Information and Resources for Small Medical Offices. (http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_SmallOffices.pdf)	This resource provides 11 security responsibilities of a practice's IT service provider(s). They can be discussed with service providers and built into contractual agreements. (Source: eHealth Ontario)	
				Information Technology Service Providers' duties – pages 9-10 of the Guide to the Personal Health Information Protection Act. (http://www.ipc.on.ca/images/resources/hguide-e.pdf)	This resource provides a description of the duties of IT Service Providers, along with a list of responsibilities that it must fulfill. These responsibilities should be included in contractual discussions and documentation; they should also be enforced and evaluated. (Source: Information Privacy Commissioner/Ontario)	
				Personal Health Information: A Practical Tool for Physicians Transitioning from Paper-Based Records to Electronic Health Records. (http://www.ipc.on.ca/images/Resources/phipa-toolforphysicians.pdf)	A section called "Health Information Network Providers" starts on page 13 of this document. It lists requirements of HINPs that should be discussed, included in contractual agreements and enforced on an ongoing basis.	

Appendix A: General Privacy & Security Checklist

Provisions	Evaluation			Information and Tools for Enhancement		
	Yes	Somewhat	No	Useful tools	Description	Comments and Additional Considerations
Information Security						
7. The work environment is safe and secure in protecting PHI.	☐	☐	☐	Quick Reference Guide to Information Security Best Practices – within the Guide to Information Security for the Health Care Sector: Information and Resources for Small Medical Offices. (http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_SmallOffices.pdf)	This is a 4-page document that provides guidelines and steps on the topics of security in all places, mobile computing, clear desk and environment, password guidelines, email information protection and security incidents. (Source: eHealth Ontario)	These can be incorporated into educational materials, policies, procedures and practices in an office. As well they provide the bases for service agreements and contracts with service and product vendors.
				OntarioMD Privacy & Encryption Tutorial (https://www.ontariomd.ca/idc/groups/public/documents/omd_file_content_item/omd011555.swf)	This is an online tutorial developed by OntarioMD that provides an overview of privacy and encryption.	
				Presentation - Protecting Personal Health Information on Mobile and Portable Devices. (http://www.ipc.on.ca/site_documents/Stop%20Think%20Protect_slides.pdf)	This is a presentation that practice can use to educate their staff on protecting personal health information when using mobile and portable devices. (Source: Information Privacy Commissioner/Ontario)	
				Fact Sheet: Health-Care Requirement for Strong Encryption (http://www.ipc.on.ca/images/WhatsNew/fact-16-e_1.pdf)	This paper this paper provides a working definition of "strong encryption" and discusses the minimum functional and technical requirements of what may be considered to be strong encryption in a health-care environment. This can be used as procurement criteria for services and equipment as appropriate. (Source: Information Privacy Commissioner/Ontario)	

Appendix B: Additional Resources

Legislation

Personal Health Information Protection Act, 2004. Service Ontario e-laws.
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm#BK5

Home Care and Community Services Act, 1994. Service Ontario e-laws.
http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_94l26_e.htm

Additional Information and Guides

Personal Health Information Protection Act, 2004: An Overview for Health Information Custodians.
http://www.health.gov.on.ca/english/providers/legislation/priv_legislation/info_custodians.pdf

COACH (Canada's Health Informatics Association). 2009 Guidelines for the Protection of Health Information.
Available for purchase here:
https://coachorg.com/en/publications/guidelinesbackground.asp

Information and Privacy Commissioner of Ontario. A Guide to the Personal Health Information Protection Act.
http://www.ipc.on.ca/images/resources/hguide-e.pdf

Information and Privacy Commissioner of Ontario. Personal Health Information: A Practical
Tool for Physicians Transitioning from Paper-Based Records to Electronic Health Records.
http://www.ipc.on.ca/images/Resources/phipa-toolforphysicians.pdf

Handling a Privacy Breach

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

Appendix B: Additional Resources

Privacy and Security with Electronic Records

COACH (Canada's Health Informatics Association). Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records. Available for purchase here: https://secure.coachorg.com/default.asp?id=1271&new=1

Information and Privacy Commissioner of Ontario. Physicians Transitioning from Paper-Based Records to Electronic Health Records. http://www.ipc.on.ca/images/Resources/phipa-toolforphysicians.pdf. May 2009

Protecting PHI on Mobile Devices

OntarioMD Privacy & Encryption Tutorial.
https://www.ontariomd.ca/idc/groups/public/documents/omd_file_content_item/omd011555.swf

Information and Privacy Commissioner of Ontario. Protecting Personal Health Information on Mobile and Portable Devices (Guidance from the Information and Privacy Commissioner of Ontario).
http://www.ipc.on.ca/site_documents/Stop%20Think%20Protect_slides.pdf

Information and Privacy Commissioner of Ontario. Fact Sheet: Encrypting Personal Health Information on Mobile Devices.
http://www.ipc.on.ca/images/Resources/up-fact_12e.pdf

Information and Privacy Commissioner of Ontario. Safeguarding Privacy in a Mobile Workplace.
http://www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf

IPC Order HO-007 (Health Order - Encrypt Your Mobile Devices, Do It Now: Commissioner Cavoukian). January 2010.
http://www.ipc.on.ca/english/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=8367

Appendix B: Additional Resources

Information for Patients

Government of Ontario. Your Health Information: Your Rights. Your Guide to the Personal Health Information Protection Act, 2004.
http://www.health.gov.on.ca/english/providers/legislation/priv_legislation/phipa_brochures/phipa_brochure.pdf