Guide to INFORMATION SECURITY FOR THE HEALTH CARE SECTOR

Information and Resources for

Small Medical Offices

Introduction

The *Personal Health Information Protection Act, 2004* (PHIPA) is Ontario's health-specific privacy legislation. PHIPA governs the manner in which personal health information (PHI) may be collected, used and disclosed within the health care system. While all staff play a role in information protection, PHIPA makes health care practitioners responsible for information security in their role as Health Information Custodians (HICs) or agents of Health Information Custodians[1]. This guide is intended for use by you, the physician and clinician, to assist in building an information security program for your community based offices. It is intended to provide assistance to manage the security of your information and create a common security practice to safeguard PHI.

To build an information security program in your office, you need to develop a security policy; define roles and responsibilities for information protection; ensure that all staff are trained and monitor compliance with the policy; and, be prepared to deal with unexpected incidents. The guide contains a description of roles related to protection of PHI as well as individual responsibilities for each of the identified roles. It includes sample documents such as a security policy, confidentiality agreement and a brochure of common best security practices.

ROLES **Information Security best practices include the designation of individuals with roles and responsibilities to ensure that information assets under their care are adequately protected. In community- based offices, there could be several roles relevant to the protection of PHI and in some cases, the same person may play multiple roles.**

Health Information Custodian (HIC)

The health care practitioner or person who operates a group practice of health care practioners is considered a HIC under PHIPA[2]. In most circumstances, physicians in community based practices are HICs. The HIC must implement reasonable physical, technical and administrative measures to safeguard PHI.

Among other obligations, the HIC must take reasonable steps to ensure the PHI in their control or custody is:

- accurate and up-to-date for the purposes for which the information is used;
- protected against theft, loss and unauthorized use or disclosure;
- protected against unauthorized copying, modification or disposal; and,
- retained, transferred and disposed of in a secure manner.

The HIC must notify patients as soon as possible if the patient's PHI is stolen, lost or accessed by unauthorized persons.

Security Officer

Staff member appointed by the physician with overall responsibility to manage the security program on a day-to-day basis. In an office setting, a security officer can be the nurse, medical office assistant or other health care professional.

IT Service Provider

An individual or a company providing IT services to the medical office, such as installing and servicing computers, installing new software and providing network connectivity.

All Staff

While there are designated roles with specific responsibilities to protect PHI, all staff that access PHI also have obligations.

[1] If you are uncertain about your role as a Health Information Custodian (HIC) or agent under PHIPA, please refer to the legislation which can be found at http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm . The website of the Information and Privacy Commissioner of Ontario, http://www.ipc.on.ca also provides resources for healthcare providers.

[2] PHIPA 3.(1)2.

Navigating the Guide

The following are components of the guide designed to be created or used by individuals in varying roles.

Health Information Custodian

Security Policy

A simplified sample policy that sets requirements, assigns responsibilities and demonstrates the physician's commitment to protecting PHI.

Staff Security Responsibilities and Confidentiality Agreement

A sample agreement to be read, understood and signed by all staff, acknowledging their individual responsibilities prior to being granted access to confidential information.

Security Officer

Security Officer Responsibilities

A list of key responsibilities for the person assigned to manage information security in the office.

Staff Security Responsibilities

A list of key responsibilities applicable to all medical and administrative staff in the office that may have access to PHI.

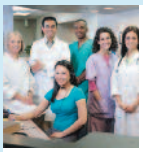
IT Service Provider

IT Service Provider Security Responsibilities

A list of minimum security responsibilities that an IT service provider needs to comply with, while providing technical services to the office.

Security Acknowledgement and Confidentiality Agreement

A sample agreement to be read, understood and signed by all staff and those managing and operating information resources that contain confidential information, acknowledging their individual responsibilities prior to being granted access to confidential information.



All Staff

Security Policy

Read the policy that sets requirements assigns responsibilities and demonstrates the physician's commitment to protecting PHI.

Security Acknowledgement and Confidentiality Agreement

Read, understand and sign by all staff, acknowledging their individual responsibilities prior to being granted access to confidential information.

Staff Security Responsibilities

A list of key responsibilities applicable to all medical and administrative staff in the office that may have access to PHI.

Quick Reference Guide

A guide to simple best practices in information security that cover the key physical, technical and administrative safeguards to protect information.

Staff Security Responsibilities

- Read and comply with the security policy.
- Read, sign, and comply with the Security Acknowledgement and Confidentiality Agreement.
- Read and follow the best practices for security in the Quick Reference Guide to Information Security Best Practices.
- Follow clean desk practices especially in unattended workspaces. Refer to Clean Desk and Environment in Quick Reference Guide to Information Security Best Practices.
- Lock filing cabinets, when unattended, and secure mobile computing devices such as laptops.
- Question unfamiliar individuals entering restricted areas.
- Secure information and computers used outside the office as per the IPC fact sheet Encrypting Personal Health Information on Mobile Devices[3].
- Avoid accidentally exposing sensitive information through conversations, exposed computer screens and unattended desks.
- Dispose of hard copy personal health information and digital media as per IPC fact sheet "Secure Destruction of Personal and Personal Health Information."
- Before sending a fax, confirm the number is still valid and was dialed correctly. Find additional best practices in IPC document Guidelines on Facsimile Transmission Security.
- Report all security incidents to the security officer.

[3] http://www.ipc.on.ca

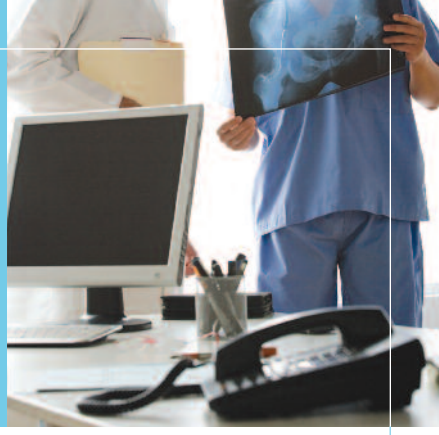
Security Officer Responsibilities

- Ensure the security policy is posted in a prominent place within the office so that it is available to both staff and patients.
- Ensure staff and contractors are aware of the security policy and informed on how it should be interpreted and put into action through support following the Quick Reference Guide to Information Security Best Practices.
- Ensure all staff are trained on their security responsibilities. Refer to Staff Security Responsibilities and Quick Reference Guide to Information Security Best Practices.
- Collect and file the signed and dated Security Acknowledgement and Confidentiality Agreement from all staff and IT Service Provider.
- Ensure disposal of personal and personal health information meets security standards as given in the IPC fact sheet Secure Destruction of Personal and Personal Health Information.[4]
- Ensure staff have access to a shredding machine to securely dispose of personal health information no longer required.
- Instruct staff how to create strong passwords, one that is easy to remember but difficult to guess, and never to share their passwords. Refer to the Password Guidelines in Quick Reference Guide to Information Security Best Practices.
- Ensure staff understand that they are not to install unauthorized software, connect unauthorized devices to their computers, or use their computers for unauthorized purposes.
- Make certain that all staff members make weekly backups of their data. If possible, keep the backups offsite.
- Revoke or suitably adjust (physical, network, system and application) access and change shared passwords as soon as employees leave or change responsibilities.
- Direct the IT service provider to set up security safeguards on all office computers including strong encryption[5], security patches and antivirus solutions.
- Ensure the IT service provider provides a written description of the service provided.
- Report all security incidents to the Health Information Custodian. Arrange assistance in leading the investigation, if necessary, and ensure required remediation is completed.
- Monitor and perform spot checks on a regular basis to ensure all staff are following the Security Policy. Take appropriate action if not followed.

[4] http://www.ipc.on.ca

[5] Refer to the IPC Fact Sheet Health_Care Requirement for Strong Encryption at http://www.ipc.on.ca.

IT Service Provider Responsibilities



- Sign agreement with the practice prior to access to confidential information, where applicable.
- Read the security policy and sign the Security Acknowledgement and Confidentiality Agreement before starting any work.
- Locate computer(s) in a secure location to minimize the risks of modification, loss, access, theft, view and disclosure by unauthorized individuals,
- Ensure each computer user is provided with a unique user ID and selects their own password.
- Instruct staff members to use strong passwords that are 8–10 characters long and are a combination of uppercase and lowercase letters, numbers and special characters.
- Enable security features such as passwords and a locked screen saver.
- Install and manage hard drive encryption, where applicable. Refer to the IPC fact sheet *Health Care Requirements for Strong Encryption.*[6]
- Install security software such as anti-virus, anti-spam, anti-spyware and personal firewall from a reputable vendor and keeping them up- to- date.
- Apply security patches and updates to computers on a regular basis.
- Connect the computers to an uninterruptable power supply (UPS).
- Ensure the security officer responsible for the overall office security understand the security features installed and what actions to take in case of an incident.

Notes: In addition to IT Service Provider Responsibilities, this is also intended to provide direction to the security officer when overseeing a third party with whom the health care practitioner or group practice intends to contract to provide IT support.

[6] http://www.ipc.on.ca

Sample

Our Security Policy

It is our office's policy to protect the personal and personal health information of all our patients in accordance with legal obligations set out in Ontario's *Personal Health Information Protection Act* (PHIPA) and in accordance with good business practices and privacy and security best practices.

Specifically, it is our policy to:

1. Protect patient or client personal information and personal health information against theft, loss and unauthorized collection, use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.
2. Comply with legislative and regulatory requirements.
3. Identify and appoint a designated security officer.
4. Ensure staff understand their responsibilities and ensure that they receive appropriate training to discharge those responsibilities.
5. Provide reference material for staff with practical security practices in key areas affecting the operations of our office.
6. Perform periodic reviews of security practices.
7. Prominently post the security policy for ready access by both staff and our patients.
8. Enter into contractual agreements with security commitments with any third party that may handle personal information and personal health information.

Clinician's signature: _____

Print name: _____

Date: _____

Sample

Security Acknowledgement and Confidentiality Agreement

In consideration of working at this office, I acknowledge the importance of protecting the confidentiality and integrity of any personal or personal health information[7] to which I have access. I agree not to collect, use or disclose such information to any person or organization except as necessary in the course of providing my services.

Further, I:

i. acknowledge that I received, read and understood this office's security policy

ii. acknowledge that I received, read and understood the Security Quick Reference Guide, as well as a statement of my own responsibilities with regard to protecting the confidentiality of information

iii. agree that this office's policy and supporting instructions form part of my terms of employment or my contract, and that any violation of this Security Acknowledgement and Confidentiality Agreement may result in disciplinary action, up to and including termination of my employment or contract

iv. agree that I will immediately notify the person with overall responsibility for security in the office in the event that I become aware of any violation of this office's security policy, or accompanying instructions, including any unauthorized collection, use, disclosure, or disposal of personal health information, other than in accordance with this office's Security Policy, as amended from time to time.

Employee's signature: _____

Print name: _____

Date: _____

[7] For the purposes of this Security Acknowledgement and Confidentiality Agreement, personal health information has the same meaning as personal health information defined in section 4 of the *Personal Health Information Protection Act, 2004* (PHIPA).

eHealth Ontario

P.O. Box 148, 777 Bay Street
Suite 701, Toronto, Ontario M5G 2C8
Tel: (416) - 586 - 6500
Fax: (416) - 586 - 4363

Toll free: 1 - 888 - 441 - 7742
Email: info@ehealthontario.on.ca
Web: www.ehealthontario.on.ca

Quick Reference Guide to

Information Security Best Practices

1 The Basics

Information security as it relates to health information is the safeguarding of personal health information (PHI). The following are guidelines on how to maintain a safe and secure work environment.

Core principles of information security:

- **Confidentiality** – ensuring that PHI is made available or disclosed only to authorized individuals.
- **Integrity** – making certain that PHI is accurate, complete and remains valid over time.
- **Availability** – ensuring information is accessible to authorized individuals when and where required.

2 Security in all Places

Printers, Photocopiers and Fax Machines

- Locate printers and fax machines in an area that is accessible by authorized staff only.
- If you print something, retrieve it from the printer immediately.
- If you fax something, confirm the number is still valid and verify that it was dialed correctly, refer to the IPC Guidelines on Facsimile Transmission Security.[1]
- Periodically review fax numbers stored in the speed dial and ensure that they are still valid.
- If you are expecting something by fax, especially if it is sensitive, treat it like a meeting: set a specific time to receive it.[2]
- Do not leave original material in photocopiers or fax machines.[3]

On the Phone

- Know to whom you are disclosing information. If uncertain, ask them to provide you with information that would verify their identity.
- Be aware of your surroundings, including cell phone conversations. Be mindful of eavesdropping.
- Be aware that there are techniques used to manipulate people into performing actions or divulging confidential information over the phone.

In Meeting Areas

- Clean the whiteboard of sensitive information when the meeting is over.
- After a meeting, double check that sensitive information including documents are removed from the meeting room.
- At the beginning of a conference call, ask all participants to identify themselves.
- After a conference call or phone meeting, check that the phone line is closed after the meeting.

3 Mobile Computing

- Ensure your laptop and personal digital assistant (PDA) are encrypted and/or password protected.
- Never leave your laptop/PDA items in view in the car.
- Never leave your laptop/PDA items or mobile phone unattended when travelling or in any other public place.
- If your computer uses wireless connections, ensure that all wireless communications are encrypted.
- When using CDs for data backup, store the files only in encrypted format. File encryption tools are provided in Microsoft Office applications. Refer to the IPC fact sheet Encrypting Personal Health Information on Mobile Devices.
- When using USB memory devices (USB flash drives) for backup or to move PHI between computers, use only devices that have built-in encryption and require a password to access information. Refer to the IPC fact sheet Encrypting Personal Health Information on Mobile Devices.
- Use power-on passwords – a password that must be entered before the device will start.
- When using a laptop outside of the office environment, ensure that your screen cannot be viewed by anyone other than you.

[1] www.ipc.on.ca

[2] Reliable security features are not common in most fax machines and do not meet standards for protecting sensitive information.

[3] www.ipc.on.ca

4 Clear Desk and Environment

- When away from the office, sensitive information (paper files and computer media) should be locked in secure cabinets. Do not leave materials unattended in open, unsecured areas such as printers, copy machines, fax machines or meeting rooms
- All sensitive information for disposal should be destroyed or erased in a secure way. Do not place them in a blue recycling bin or garbage. Refer to the IPC fact sheet *Secure Destruction of Personal Information*.[4]
- Incoming and outgoing mail and fax should be stored in a secure location.
- Avoid removing sensitive documents and data from business premises, unless necessary.

5 Password Guidelines

- Ensure that your computer has a screen saver that activates after a predefined time and requires a password to gain access to the computer.
- Change your passwords frequently, at least every 90 days.
- Passwords must NEVER be disclosed to anyone or written down.
- A password must have the following characteristics:
  - contain a minimum of eight characters
  - include a combination of upper and lower case letters, numbers and/or special characters, e.g. #, ~.
  - Should not be obvious, easily guessable, or found in a common words dictionary should not use acronyms, birthdays, sequential numbers, names of family members or pets.
- If you suspect the confidentiality of your password has been compromised, change it immediately.

6 Email Dos and Don'ts

Do:

- Use appropriate signatures and standard disclaimers on email messages, faxes and other documents.
- Be aware of techniques used by lawbreakers in attempt to gather personal information from you via email. For example, you may receive an email request to send lab results or provide other health or financial information from a user unknown to you.
  - Carefully address emails. Always double-check the name(s) in all the address lines
  - Be cautious about communicating sensitive information via email using mobile electronic devices (i.e. personal digital assistants) in public places where third parties may eavesdrop on the communication.

Don't

- Forward sensitive materials from your office email to your personal email address such as Hotmail, Yahoo! and/or Gmail. The security level of these personal email accounts is weak and susceptible to compromise.
- Open email messages and attachments from senders you don't recognize and trust.
- If you suspect or know that an email message contains a virus, do not forward the email message.
- Reply to spam email, also known as junk email or unsolicited email.
- Click on links within spam email.

[4] http://www.ipc.on.ca

7 How to Protect Information

- Understand security as it relates to your role and your obligations.
- If your workplace requires a badge, wear it at work. Question anyone without a badge and ensure that visitors in secure or sensitive areas are escorted at all times.
- Where applicable, be aware of unauthorized physical access to premises through piggybacking, this is when an individual without a badge will follow an authorized employee onto the premises.
- Select strong passwords and protect them from disclosure.
- Always lock your screen when you are away from your computer.
- Never use another person's user ID or password.
- Scan your computer weekly to ensure that spyware or unauthorized software is not installed.
- Make weekly backups of your data and keep the backups securely offsite.
- Install a privacy screen over your monitor to make it difficult for casual visitors in your office to read the contents displayed.
- Verify at least twice a year that you can restore data from backup disks or tapes.
- Secure laptops with a physical cable lock when in use.
- Request that your computer's hard drive be encrypted.
- Do not install unauthorized software of any kind.
- Never visit websites intended for adult-only audiences, gambling or online games.
- Keep all paper files, backup CDs and/or tapes in a fireproof cabinet.

8 Security Incidents

What is a security incident?

A security incident is an unwanted or unexpected situation that results in:

- The unauthorized disclosure, destruction, modification or withholding of information.
- A failure to comply with the organization's security requirements.
- Unauthorized access, use or probing of information resources.
- An attempted, suspected or actual security compromise.
- Waste, fraud, abuse, theft, loss of or damage to resources.

Why might they happen?

- Failure to comply with approved policies and practices.
- Indifference to or being unaware of responsibilities.
- Inadequate, or lack of, safeguards.

What are possible consequences?

Damage to reputation, loss of trust, financial losses, theft of computing resources, loss of employment or legal consequences.

What do I do if I witness an incident?

Security incidents must be reported to the security officer. The security officer must take appropriate action to contain actual or potential breaches, investigate and report the finding(s).

If you experience an incident, report it to the security officer. All incidents relating to the information you are responsible for should be appropriately identified, responded to, escalated and investigated.