



# Welcome to the Privacy e-learning Module



# INTRODUCTION AND INSTRUCTIONS



*Privacy is a **legal** requirement,  
a **professional standard**,  
and an **ethical obligation**.*

*More importantly, privacy is critical to maintaining strong relationships with patients, who trust that the BCHS will use the Personal Health Information to make an accurate diagnosis and plan effective treatment.*

This course takes approximately 20 minutes to complete and will cover basic steps you can take during your daily routine to protect privacy.

There is a brief quiz at the end of this learning module.

This is a **mandatory** e-learning module and **MUST** be completed by all employees on an annual basis. Compliance will be monitored and followed up on.

# Key Concepts:

Ontario's ***Personal Health Information Protection Act*** (***PHIPA*** – ***pronounced P-HIPA***) defines how personal health information may be handled.

The *Act* governs:

- ***collection, use*** and ***disclosure*** of personal health information (PHI), for health care and secondary purposes

PHIPA builds on other laws like the *Public Hospitals Act* in setting out the obligations of all staff, physicians, students and volunteers working on behalf of the hospital to protect patients' personal health information

# What is **Personal Health Information (PHI)**?

PHI is information about an individual that:

- identifies a person, and connects that person to receiving care at the BCHS
- PHI can be found in many forms, including:
  - on paper (e.g. charts, printouts, messages and notes)
  - in electronic files (e.g. electronic charts, letters, spreadsheets, emails)
  - in conversations with patients

# Access and Exposure to PHI:

You are responsible for protecting PHI in all forms

As a member of BCHS staff who supports the provision of care, you may have **access to PHI** or be **exposed to PHI** in a number of different ways, including (but not limited to):

- accessing PHI to support patient care (e.g. chart creation, billing) or business operations (e.g. quality improvement, technical support)
- using PHI to follow up on appointments or administrative tasks

## **Access and Exposure to PHI Cont'd.:**

- responding to requests to release PHI outside the hospital
- filing, transporting or otherwise handling patient records
- interacting with patients (e.g. responding to, directing, transporting, or otherwise supporting patients)
- overhearing conversations with or about patients

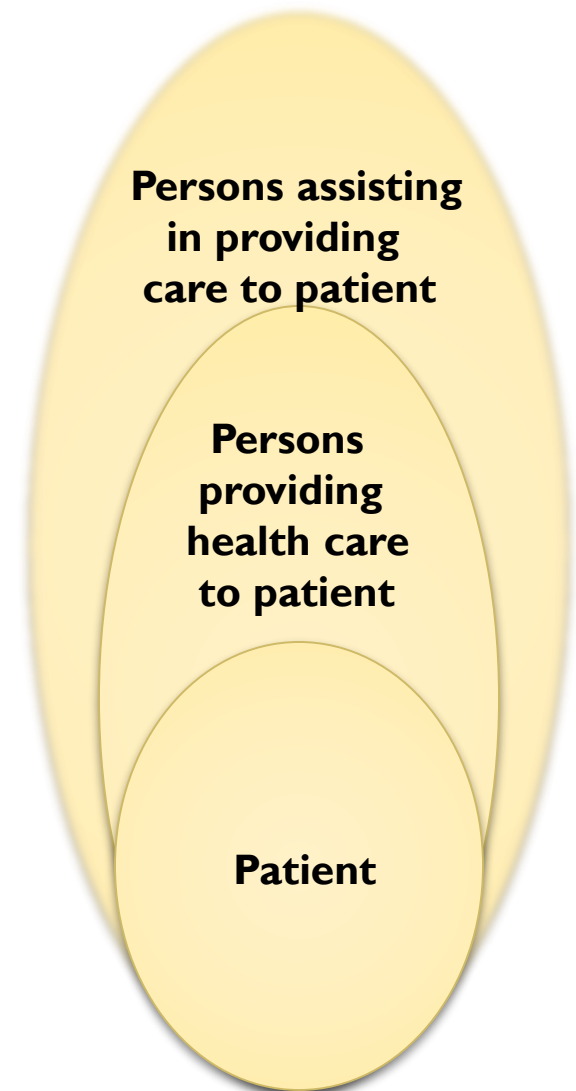
# ***“Circle of Care”***

***Sharing information within  
the circle of care***

Together, the patient’s clinicians are informally called the **“circle of care”**.

Staff and volunteers who provide direct patient care are also permitted to access and use PHI to complete their tasks.

## **Circle of Care**





# ***“Circle of Care”***

## ***Sharing information within the circle of care cont’d***

- **You can assume consent to share PHI with other hospital personnel** if needed to:
  - support patient care (including with physicians, nurses, allied health staff, lab and radiology staff, students, volunteers, administrative staff, or others providing or supporting care)

## ***“Circle of Care”***

***Sharing information within the circle of care  
cont’d.***

- PHI may also be shared (disclosed) with patient’s **external care providers** (including a GP, referring MD at another hospital, laboratory, rehabilitation centre, CCAC, long term care facility) if:
  - they will use the information to provide direct care and if the patient has not **explicitly** told us not to share their information

# How can you protect privacy while performing your daily tasks?

Accessing PHI appropriately. If accessing patient records, ***mind your business***



- Only access the records and information you need to perform the duties of your job
- Unauthorized removal of PHI from BCHS is not permitted
- Do not access information about friends, family, co-workers, or anyone of interest
- Routine audits are conducted on access to records with disciplinary actions for privacy breaches, which could include **termination**

# How can you protect privacy while performing your daily tasks cont'd.

- Do not share login information
- **Log out** from your computer
  - You are responsible for any activity that occurs under your login
- Do not access PHI at the request of another staff member.

# Sharing PHI outside the “Circle of Care”

All third party requests for personal health information must be directed to Health Information Services – Release of Information

- patients’ lawyers, employers, insurers
- patients’ friends and family
- external providers who want to use PHI for non-care purposes (e.g. quality improvement)
- BCHS members who would like to request their own personal health information

# **When can I disclose PHI *without* expressed consent?**

You may disclose PHI without expressed (verbal or written) or implied consent (even if the patient has told you not to share their information) if PHIPA or another law permits or requires a specific disclosure, such as:

- Child abuse (Child and Family Services Act)
- Significant risk of harm (PHIPA)
- Gun shots wounds (Mandatory Gunshot Wounds Reporting Act)
- Reportable Diseases to Public Health (Health Protection and Promotion Act)

# What can I tell callers and visitors?

*Unless the patient has told you not to (and there is no concern about safety or another known exception), you can tell callers and visitors:*

- Conditional status, presence and patient location may be provided to those outside of the circle of care
  - *Conditional status includes, “good, fair, poor, serious”*
- Additional information requires the patient’s expressed consent

# Conversing Carefully:

Don't discuss confidential information in public areas of the hospital (e.g. elevators, cafeteria) or in the community (e.g. on public transportation, in the shopping mall or at home)

***Remember to ask patients for their consent before...***



- giving detailed updates to patients' family or friends
- leaving a detailed voicemail
- asking the Substitute Decision Maker if the patient is incapable of making a decision about their information



# Using Electronic Files and Devices:

- Save files to a **hospital network drive**, not to your computer's hard drive
- **Do not save files with PHI to a personal device (e.g. Blackberry)** without approval
- Lock up or hand off devices when leaving them unattended
- Ensure you have your devices with you when leaving a public space (e.g. cab, meeting place)

# Using Electronic Files and Devices

## Cont'd.

- You may only save files and emails with PHI to an approved **portable device** (e.g. Laptop, USB key, or PDA) if absolutely necessary as part of your role and:
  - only the minimum amount of PHI is copied
  - the device is encrypted
  - files are deleted from the device when no longer needed

# Information Security and Media:

- Do not post confidential information on personal or public websites, e.g. social media



Potential to  
expose PHI

- As per BCHS policy, do not take photographs, video record and/or sound record patients unless you have the appropriate consent

Reference: BCHS Policy and Procedure  
[Cellular Phones.docx](#)

# Storing and Disposing of Paper:

- File all clinical information in patients' charts
- Lock up paper records when unattended
- Shred unwanted paper or place in shredding bin (including print-outs from patient records, patient lists, and appointment and schedules)
- Do not use the back of paper with PHI as note/scratch pads
- Report any loss or theft of paper or electronic devices *immediately* to your supervisor



# Using Email:

If sending an email containing PHI to an **authorized recipient** (e.g. a patient's care provider):

- Care providers must obtain consent for email correspondence prior to communicating via e-mail
  - Consent may be obtained in person at the time of a patient's appointment, or through e-mail if the patient expresses his/her consent in a return e-mail from the care provider

Reference: BCHS Policy and Procedure  
[email storage and retention.docx](#)

# Using Email Cont'd.

If a patient emails you requesting an emailed response:

1. Inform the patient's clinician of the request and confirm the appropriate response
2. Communicate the risks of using email to the patient. A consent form obtained from the Privacy Office must be signed (in verbal conversation or by replying with a disclaimer)
3. Wait for patient's confirmation that they accept the terms/risks
4. Document on chart that consent was received or add a signed consent form to the chart

# Email Safety:

If emailing from or to an approved address or emailing to an unapproved address with patient consent:

- Only include the minimum amount of PHI necessary
- Do not put any PHI in the subject heading
- When forwarding and responding to emails, ensure there is no reference to other patients
- Double check the recipient's address

# Reporting Incidents:

Under PHIPA and hospital policy, patients must be notified if their PHI is lost, stolen, or inappropriately accessed, used or disclosed (including if PHI is sent to someone not allowed to receive it or seen by someone not allowed to see it)

These situations are privacy **incidents** and must be reported immediately.

How can you report an incident?

- inform your Supervisor/Manager (Risk Pro report)
- inform the Privacy Officer



# Unauthorized Access:

*Within PHIPA there is an obligation by hospitals to ensure the personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure*

**Any unauthorized viewing of the personal health information constitutes a privacy breach**


The following has come into force under PHIPA related to Privacy breaches

- Prosecutions can result for wilful collection, use or disclosure of personal health information in contravention of PHIPA or its regulations and fines for privacy offences of \$100,000 for individuals and \$500,000 for organizations.
- Mandatory Reporting to Regulatory Colleges for employee who is terminated, suspended, or subject to disciplinary action resulting from the unauthorized collection, use, disclosure
- Notification to an affected individual of a privacy breach to include include a statement that the individual is entitled to make a complaint to the Office of the Information and Privacy Commissioner/Ontario (the IPC).

# Hospital workers convicted for snooping into Rob Ford's personal health files

Pair at Princess Margaret Cancer Centre, who pleaded guilty, are the first ever convicted under Ontario's health privacy act.



Jun 17, 2016 | Vote  0  0

# 397 medical records snooped at Hamilton General Hospital

Hamilton Spectator

By Joanna Frketich 

An employee snooped into the medical records of 397 patients at Hamilton General Hospital.

The staff member was fired after an investigation by Hamilton Health Sciences concluded the privacy of emergency room patients was breached from June 2015 to May 2016.

"There's no evidence that there was any malicious intent or use of the information," said Dave McCaig, executive vice-president of corporate affairs. "It was a case of curiosity."

Registered letters started going out this week to patients involved.

"All patients have been informed," McCaig said.



## GENERAL

Kaz Novak, The Hamilton Spectator file photo

*A member of staff at General Hospital has been fired after snooping into almost 400 medical records.*

# **Accessing your own Personal Health Information at BCHS**

All individuals have the right to request their Personal Health Information. The PHI belongs to you, however, it is in the care and custody of BCHS.

To request your PHI you will need to make a formal request to Release of Information (ROI) which will require:

- A valid consent
- Photo identification
- Prepayment of ROI fee

ROI reviews the request and responds within 30 days

FAQ and contact information can be found on our website at [www.bchsys.org/hospital/about-us/accountabil/personal-health-records/?cID=4971](http://www.bchsys.org/hospital/about-us/accountabil/personal-health-records/?cID=4971)

# Role of the Privacy Officer

- advocate for patient and staff privacy within the organization
- develops privacy related policies and processes
- conducts internal audits of health records and the organization's processes to ensure compliance
- The Privacy Officer can be reached by calling Ext. 2556.





## Confidentiality Agreement

All employees/physicians/volunteers/students and staff from external agencies who have access to confidential information concerning patients, hospital personnel and hospital business are directed by the Brant Community Healthcare System Statement of Information Practices and are required to sign this *Confidentiality Agreement*, on an annual basis.

In my affiliation with Brant Community Healthcare System, I understand that:

- Brant Community Healthcare System has policies and procedures with respect to privacy, confidentiality, and security and it is my responsibility to be familiar with the requirements outlined in such policies and procedures.
- I will not use Brant Community Healthcare System information or communication systems to access confidential information unless legally authorized to do so and as required in the proper and faithful discharge of my duties or responsibilities
- Except when I am legally authorized to do so and as required in the proper and faithful discharge of my duties or responsibilities, I will not access, use or disclose confidential information that comes to my knowledge or possession by reason of my employment or affiliation with Brant Community Healthcare System.
- My handling of confidential information may be subject to monitoring and audit activities.
- I will not share my access codes (eg. my computer password, voicemail password, pin number for door locks, pin for electronic signature).
- I have a responsibility to assist other persons employed or affiliated with Brant Community Healthcare System with their obligation to maintain confidentiality.
- I will not leave confidential information exposed for others to view (eg. computer screen or patient record or discuss confidential information in public areas)
- I am required to report any breach or suspected breach of confidentiality to BCHS's Privacy Office; and
- I am accountable for my actions and the consequences of my actions related to the handling of confidential information.
- ***Privacy breaches are subject to disciplinary action up to and including dismissal. Mandatory reporting to Regulatory Colleges is required for employees who are disciplined resulting from the unauthorized access, collection, use or disclosure of health information.***

Attached to this document are questions and answers that will assist you with understanding the policy. One copy of this Agreement will be retained by BCHS to become part of your personnel file, and one copy will be given to you for your personal records.

I understand that a breach of this agreement may be cause for disciplinary action including, but not limited to, written warnings or letters of counsel, suspensions with or without pay, and/or immediate termination of employment, affiliation, suspension or revocation of hospital privileges with Brant Community Healthcare System; and prosecution under the law.

<b>Print Name:</b>	<b>Signature:</b>
<b>Department:</b>	<b>Site:</b>
<b>Date:</b> (dd-mm-yyyy)	
<b>Status:</b> ( ) Employee    ( ) Medical Staff    ( ) Student    ( ) Volunteer    ( ) Other: _____	

**Thank you for completing the Privacy  
e-learning Module!**