Brant Community Healthcare System

The Willett, Paris

The Brantford General

Welcome to the FIPPA / Privacy e-learning Module

Adapted with permission from Ontario Hospital Association, 2013

What is FIPPA?

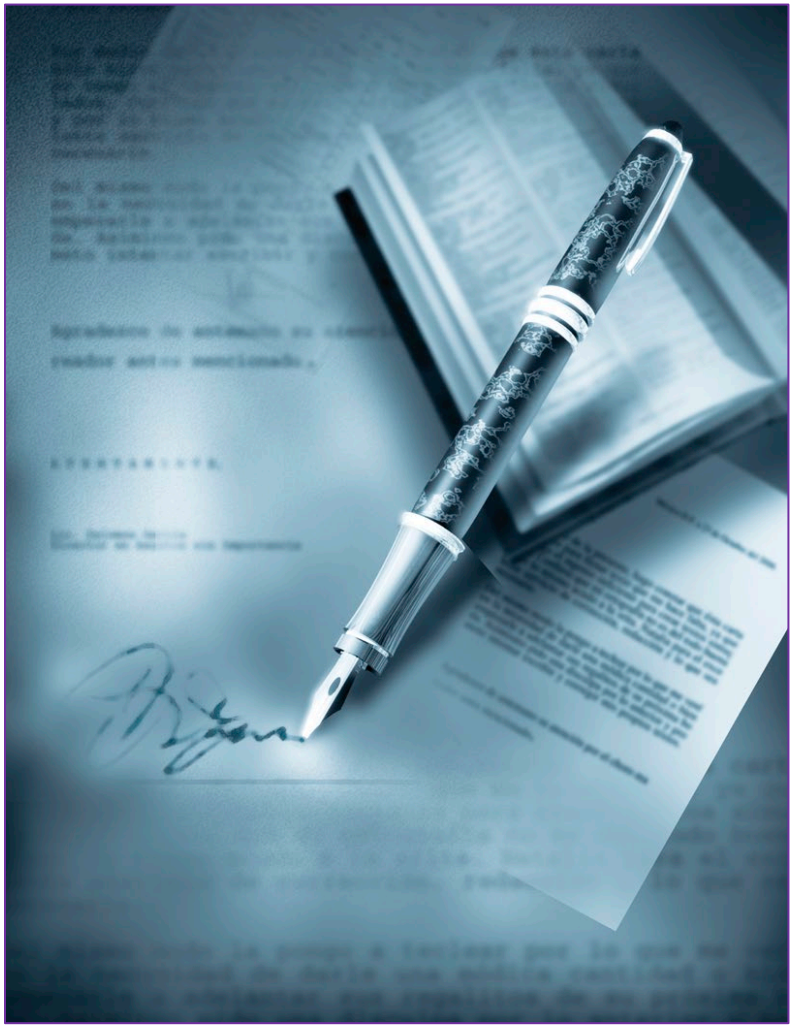
Freedom of

Information and

Protection of

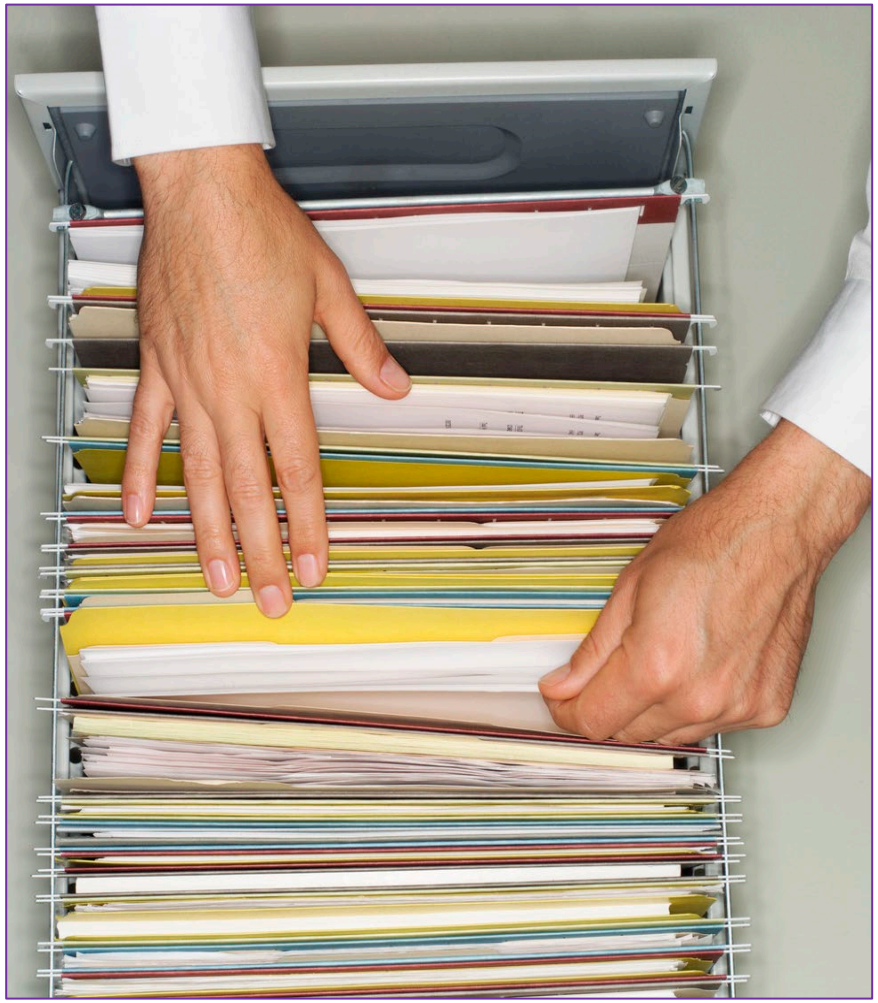
Privacy

Act



What does FIPPA do?

FIPPA provides people with a right to access information that is under the control of institutions in the public sector, such as universities and hospitals.



FOUR PRINCIPLES

Four principles form the foundation of the legislation:

1. Information should be available to the public
2. There should be exemptions to access, which should be limited and specific
3. Decisions on disclosure of information should be reviewed independently
4. The privacy of individuals and their personal information should be protected; those individuals should have access to that information on request

WHAT IS A RECORD?

A record is any reproducible document, whether on paper, video or in electronic or other format

Examples include minutes of meetings, handwritten notes, e-mails, contracts, travel expenses, interview notes, reports, business proposals, interdepartmental memos, security video, etc.

WHO CAN REQUEST RECORDS?

Anyone. Requests may come from individuals, groups, businesses or media outlets like the Brantford Expositor.

The right to access is not limited by citizenship or place of residence, so for example an international student who completed a placement at BCHS can request his or her record.

WHAT CAN THEY ASK FOR?

Anything that we have in our custody, generated on or after January 1, 2007.

There are exemptions. Foundation records (charitable donations, donor names, etc) are exempt, as are records of work done by the hospital's Quality Council under the Quality of Care Information Protection Act (QCIPA) and all records pertaining to abortion and certain Human Resources/personnel records.

HOW ARE REQUESTS MADE?

A formal request must be made in writing (not by phone) to the hospital where the person requesting the information believes the record exists.

There are two types of formal requests – personal information ("I want information pertaining to me") or general access ("I want all BCHS emergency codes procedures"). There is a cost of $5 for each request and this must be paid at the time of the request.

WHO IS RESPONSIBLE?

All formal requests are handled by the BCHS Freedom of Information & Privacy Office, supported by FIPPA leads in each department who assist with the search for requested records.

As an organization, BCHS has only 30 calendar days to respond to each request. If you receive a formal (written) request in your area, contact the FOI & Privacy office **immediately**: Ext. 2596 or foi@bchsys.org

INFORMAL REQUESTS

We often receive informal requests for information. For example, staff from another hospital may ask about our policies, procedures or strategies. This type of information is available to the public and we currently do share it with others as requested. We will continue to do so in the future. The Freedom of Information & Privacy office need not be involved.

PERSONAL INFORMATION

BCHS is legally obliged to protect personal information. Therefore, your personal information will not be released to anyone without your consent.

Personal information is recorded information about a person and includes race, family status, employment history, identifying numbers (such as employee number, Social Insurance Number) etc.

Personal information is not employee business contact information – your extension and e-mail address – as this information is in the public domain.

Only you yourself can ask for your personal information; BCHS is required by law to share that information with you, with a few limitations.

PERSONAL HEALTH INFORMATION

BCHS is legally obliged to protect personal health information under the provisions of the Personal Health Information Protection Act (PHIPA). Personal health information, including patient charting and other patient records, will not be subject to FIPPA requests.

Anyone requesting personal health information would do so under the provisions of PHIPA, which sets our strict guidelines for us to follow in the collection, use, sharing, retention and destruction of personal health information.

Remember: ***P****ersonal* ***H****ealth Information is covered by* ***PH****IPA;*

Hospital ***F****iles are covered by* ***F****IPPA*

FIPPA-FRIENDLY MINUTES

COMMITTEE MEETING MINUTES ARE SUBJECT TO FOI-FIPPA REQUESTS

When drafting your meeting minutes, always assume they will be made available to the public

WAYS TO KEEP YOUR MINUTES FIPPA-FRIENDLY

- Document the processes and outcomes of the meeting, don't record discussion word-for-word
- Include only factual and concise statements about each issue discussed, omitting unnecessary details
- Provide enough details so that a reader could trace the actions that led to a decision
- Don't include unsubstantiated or subjective information or opinions
- Protect the privacy of meeting attendees by avoiding the use of personal information without losing the meaning, importance and context of what was said.

FIPPA-FRIENDLY E-MAIL

E-MAIL FILES ARE SUBJECT TO FOI REQUESTS

WAYS TO KEEP YOUR E-MAIL FIPPA-FRIENDLY

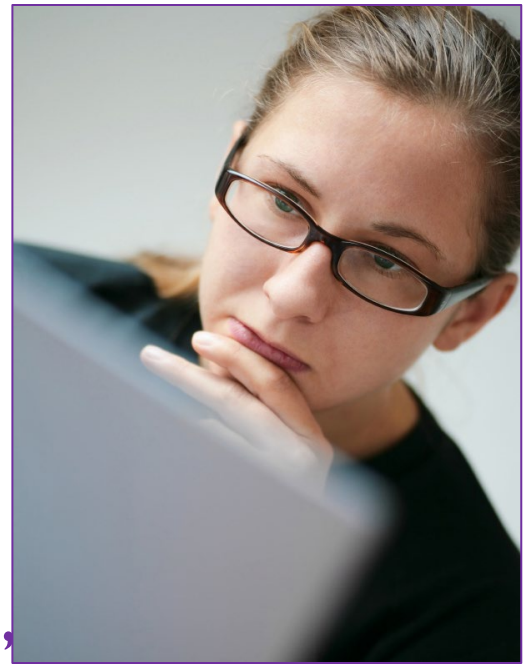
- Only send e-mails to the people who really need to see them
- Keep your personal distribution lists up-to-date
- One subject, one e-mail (and be concise and specific)
- Write content using professional language, style, tone and subject matter, avoiding abbreviations.
- Delete e-mail trails if they are not relevant or contain sensitive material.
- When replying to an email, ensure that you use 'reply all' only when others in the conversation need to hear your response.
- Try to avoid forwarding e-mails. If you must forward an e-mail, let the originator know
- Avoid using e-mail for confidential or sensitive information where possible.
- E-mail containing personal information or personal health information should be filed, secured and kept with the same care as any confidential records.

Remember: Your e-mail inbox is NOT A STORAGE CABINET for files and information!

Once you've received an e-mail, save the attachments and messages you need in the server and delete the e-mail.

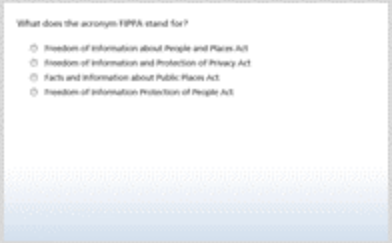
FIPPA-RELATED POLICIES

For further information about BCHS policies on FIPPA fees, processes, roles and responsibilities, as well as policies governing the creation, retention, sharing and destruction of e-mail and other kinds of records, please check our BCHS Policy Manual, which can be searched through DOCS.



QUESTIONS?

Contact our Freedom of Information & Privacy Office at Ext. 2596, or FOI@bchsys.org



FIPPA Quiz

Quiz - 10 questions

Last modified: Monday, June 19, 2023 at 12:50:47 PM

Properties

On passing, 'Finish' button:	Goes to next slide
On failing, 'Finish' button:	Goes to slide
Allow user to leave quiz:	After user has completed quiz
User may view slides after quiz:	Any time
Show quiz in menu as:	Multiple Items

Edit in Quizmaker

Edit Properties

BCHS Privacy

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.

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.:

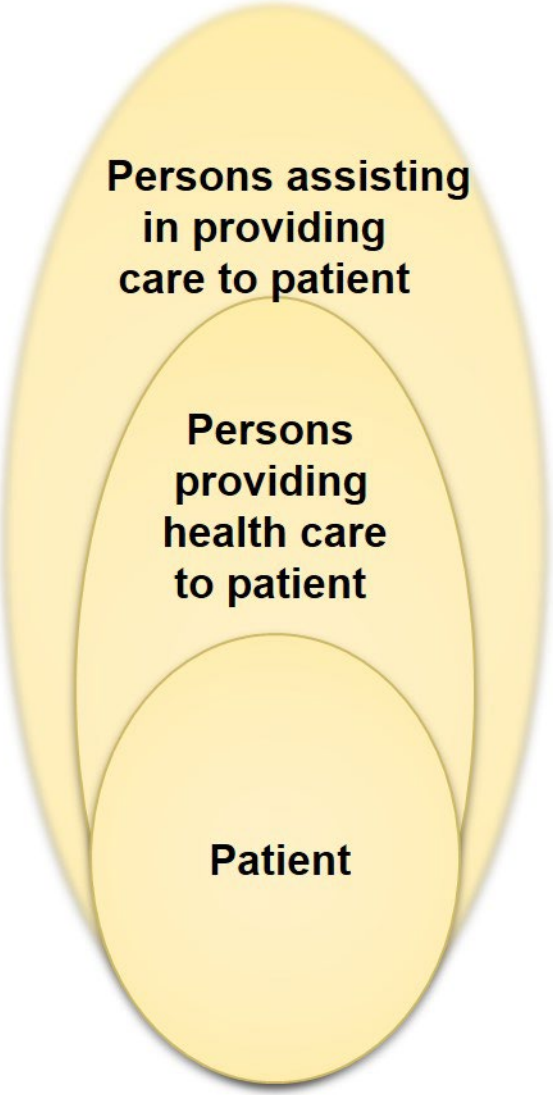
- responding to requests to release PHI outside the hospital
- filing, transporting or otherwise handling patient records
- interacting with patients (e.g. responding to, directing, transporting, or otherwise supporting patients)
- overhearing conversations with or about patients

"Circle of Care"

Sharing information <u>within</u> 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"

Sharing information <u>within</u> 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 supporting the provision of health

"Circle of Care"

Sharing information <u>within</u> 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

Reference
BCHS Policy & Procedure
Health Information Services – Release of 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

Reference
BCHS Policy & Procedure
Confidentiality of Personal Health Information

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

Ask 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. iPhone, Android)** 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
  - Do not remove original paper chart/specimens from BCHS site and electronic information only if permission given and encrypted

Information Security and Media:

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

- 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.doc

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 of theft of paper or electronic devices *immediately* to your manager

Using Email:

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

- Care providers must obtain signed 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.doc

Using Email Cont'd.

If a patient asks or emails you requesting you email their Personal Health Information(PHI)

Please refer them to BCHS
Release of Information at ext. 2483
located in the Health Information Department

Email Safety Standards to follow when approved to email PHI:

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 or faxed to someone not allowed to receive it or seen by someone not allowed to see it).

It is required that you be part of the '*Circle of Care*' to *access* or *view* patient records.

When looking up patients, apply the 'Two Identifier' rule to ensure that you are looking at the correct patient. *(name and record number, name and birth date, etc.)*

If you are requested to assist a patient, for example, who does not know where their appointment is, always ask if they have any paperwork that you can review and only as a last resort, you may access their record to assist.

You ***MUST*** immediately send an email to Privacy, identifying the patient and the reason for access.

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

How can you report an incident?

- Inform your Manager
- Inform the Privacy Officer

Reference
BCHS Policy and Procedure
Privacy Breach.doc

Unauthorized Access:

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 Information and Privacy Commissioner of Ontario (IPC) is responsible for ensuring that Health Information Custodians comply with *PHIPA*

The IPC has power to review, make rulings and issue orders to resolve complaints

April 2020 Bill 188 was passed

Fines for an individual have increased from $100,000 to **$200,000** and for an institution have increased from $500,000 to **1 million**, for committing an offence under *PHIPA*

PHIPA permits the courts to award up to $10,000 in damages for mental anguish resulting from contravention of *PHIPA*

In addition to the increased penalty, the amendments provide for the possibility of a maximum one-year term of imprisonment for a natural person guilty of an offence under PHIPA.

Auditing

- To meet compliance with PHIPA legislation, BCHS Privacy is required to have a robust auditing program of access to PHI under BCHS control and includes accesses to Clinical Connect

- **This includes Auditing Access to the following patient records:**
    - **VIP/Confidential patient**
    - **COVID or VAT patient**
    - **Discharged Patient or Expired Patient**
    - **patient that is residing on a different unit than you are working on**
    - **patient who is an employee of BCHS**
    - **Same Last Name**
    - **Same Street**
- **access to your own PHI, (Same Name)**
- **access where you keep logged on to your computer for more than 30 minutes with out any activity**
- **access when you have Excessive Log ins**
- **when you are logged in to ClinicalConnect and you open another ClinicalConnect session on another computer or browser on the same computer**
- Audits are done routinely but also when requested by patient, requested by Staff, as required during privacy investigations
- BCHS is required to audit Clinical Connect access for all of the above
- Staff are accountable for ALL their access of electronic and other forms of patient PHI and should understand that everything they access is collected and can be viewed in an audit
- Audits are done routinely but also when requested by patient, requested by Staff, as required during privacy investigations

Technology/Meditech

The proper use of the **status boards** is for reviewing patients in your circle of care who are on your floor, not other floors or patients who are not in your circle of care. (Unless your role requires you to do so)
Should you be audited, and you are not required to review another units status board, you will be flagged and an explanation will be required.

Diagnosis field on the status board – please ensure you are circle of care for a patient when clicking on the diagnosis field. The diagnosis is personal health information(PHI)) and therefore requires circle of care to access.
This field is auditable and if you are audited and are not circle of care (or your role requires you to do so) you will be flagged and an explanation will be required.

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 OR you can sign up to ConnectMyHealth to access your Personal Health Information. (healthrecordsonline.ca/register)

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.