Course Objectives

By the end of this training, you will understand:

1. Key obligations under privacy legislation (PHIPA) to protect patients’ personal health information;
2. Your role and responsibilities in maintaining privacy;
3. Privacy breaches and related consequences;
4. Obligations with respect to accessing eHealth Ontario’s shared electronic health record systems (e.g. OLIS, DI-CS, DHDR, and the ConnectingOntario ClinicalViewer), as well as TOH’s own health information systems; and
5. The limitations and processes for using and/or sharing personal health information.

Important!
There are differences in how eHealth Ontario’s shared electronic health record systems operate - those will be identified where applicable.
Why Protect Privacy?

It’s the law! It’s the right thing to do! It’s your professional obligation!

If you violate privacy or commit a privacy breach, it could cost you:

- Your position at TOH, career and reputation
- Review by a health profession regulatory college and the Information and Privacy Commissioner of Ontario
- $100,000 in personal fines
- A civil lawsuit and/or prosecution
- Retraining on privacy and security requirements
- Loss of access to one or more systems
- Significant financial losses for your organization

We all need to protect personal health information (PHI)

What if I don’t work with PHI?

We are all part of TOH, so it is important for everyone to understand how to protect PHI...

- you may find a document laying around
- you may receive a fax or e-mail in error
- you may overhear discussions in a unit conference room
- you may see a computer with someone still logged in

It is important for us all to understand how PHI must be protected.

You can also apply these techniques to respecting and protecting confidential staff information if you handle that in your role.
Why do I need Privacy and Information Security Training?

As a staff of TOH, you need to understand what activities are acceptable and what constitutes a privacy breach or security incident.

At the end of this training, you will understand your obligation to protect patient privacy as a staff member at TOH, UOHI, and OHRI.

Understanding Ontario’s Health Privacy Law

The Personal Health Information Protection Act, 2004 (PHIPA) amended in 2016, is the law that protects the privacy of an individual and the confidentiality of an individual’s personal health information.

Under PHIPA, even just viewing personal health information means you have collected and/or used it and could constitute a privacy breach.

Viewing is considered a collection or use and you are responsible under the law for protecting that information.

What PHIPA does...

PHIPA sets rules for the collection, use and disclosure of personal health information.

It also provides individuals with the right to access and request a correction of their records of personal health information.
Definition of Personal Health Information (PHI)

Personal Health Information (PHI) is all identifying information about an individual in oral or recorded form if the information relates to:

- The individual’s physical or mental health, including family health history;
- The provision of health care to the individual, including identification of the health-care provider;
- Payments or eligibility for health care, or eligibility for coverage for health care;
- Donation of body part or bodily substance;
- The individual’s health number; or
- Identification of an individual’s substitute decision-maker.

Examples of PHI:
- Provider name;
- Individual’s address and telephone number;
- Electronic medical charts;
- Lab specimens;
- X-ray results;
- Drug information; and
- Health card number and medical record number.
How Does the Law Apply to TOH and Staff?

When providing health care, each person and organization has a role under the *Personal Health Information Protection Act, 2004* (PHIPA):

**TOH’s role: Custodian**

TOH is a health information custodian and is accountable for the personal health information it collects, uses and discloses.

**Your role: Agent**

As a staff of TOH and a user of its electronic health record system, including eHealth Ontario’s shared electronic health record systems, you are an Agent. Under the law, that makes you accountable to TOH for your actions in dealing with personal health information.

Protecting Personal Health Information (PHI)

At TOH, UOHI, and OHRI, we use security safeguards to help protect personal health information against:

- loss or theft
- unauthorized access, disclosure, copying, use or modification

**Note:**

Strong administrative, physical and technical protections are also built into eHealth Ontario’s shared electronic health record systems.

For more information, refer to the Connecting Ontario Health Care Provider Guide

http://www.ehealthontario.on.ca/en/initiatives/resources

What is Ontario’s Electronic Health Record?

It enables authorized health care providers to centrally access personal health information. It includes:

- **ConnectingOntario**: clinical reports
- **Diagnostic Imaging Common Services (DI CS) Repository**: diagnostic imaging reports
- **Ontario Laboratories Information System (OLIS)**: laboratory test orders and results
- **Digital Health Drug Repository (DHDR)**

Protecting Personal Health Information (PHI)

These are the ways we can protect personal health information of TOH patients.

*Click each heading to learn more*
Physical Measures: what can you do in your environment etc?

- Locked filing cabinets
- Locked offices with restricted access
- Not leaving personal health information in unsecured areas where unauthorized personnel or members of the public could have access
- Personal health information backed-up and stored in a secure data centre
- Formalized processes and procedures for the disposal and replacement of hardware

Remember!
When working at home or at other locations outside of the hospital you must make sure personal health information and any confidential information is stored in a locked filing cabinet or drawer. It must be kept under your constant control.

Administrative Measures: what processes already exists or can be put in place in your workplace or through eHealth Ontario to protect personal health information (PHI)?

- Confirmation of identity before providing access to PHI
- Limiting access to personal health information to a “need to know basis”
- Requirements to sign agreements to protect PHI
- Awareness and Training
- Policies and Procedures
- Appointed Privacy and Information Security leads
- Privacy and Information Security Committee to oversee operational activities
- Privacy Impact Assessments and Threat Risk Assessments
Policies and Procedures are an important administrative measure. Here is where you can find them...

Find Policies or Procedures on my Hospital under the 'Policies and Procedures' tab.

OHRI and UOHI:
Follow TOH’s policies and procedures

eHealth Ontario:
eHealth Ontario’s privacy and security policies for its shared electronic health record systems can be found online at:
http://www.ehealthontario.on.ca/en/initiatives/resources
Technical Measures: What Technical Measures or Safeguards are available?

- Use of firewalls and encryption
- Strong password requirements and a rule that individuals do not share or write down those passwords
- Access controls (e.g. electronic badges to access restricted areas)
- Electronic reminders (e.g. pop-up screens)
- Users must lock or log-off their computers when they leave it
- Auditing of all systems to detect unauthorized access
- Consent directives (blocked health information) and privacy warning flags
- Search controls (open-ended searches are not allowed)
- Headers and footers with a notice of confidentiality in printouts
- ConnectingOntario users who work for more than one organization must select TOH when acting on TOH/s behalf

Remember: Staff are responsible and accountable for any unauthorized access caused by leaving their computer logged-on and unattended.

Passwords

Strong passwords generally contain 8 or more characters and a mix of numbers, special characters, and small and capital letters. Change your password if you feel it has been compromised and notify the Information Privacy Office.

Lock or Log off

If you need to leave your computer you must either:
- Lock the screen by pressing Ctrl - Alt - Del

Auditing

All your activities in TOH’s electronic health record systems and in eHealth Ontario’s shared electronic health record systems are logged, monitored and audited.

The following examples are activities that are logged and audited:
- When you login/logout
- Viewing any personal health information
- Overriding a privacy warning flag or consent directive
What are a privacy breach and an information security incident?

Be aware that a privacy breach or an information security incident can be:

- Actual or suspected
- Intentional or unintentional

- A contravention of:
  - A provision of the Personal Health Information Protection Act, 2004 or its regulations;
  - Applicable agreements’ privacy provisions;
  - Privacy policies, procedures and practices implemented;

- Personal health information is lost or stolen or has been accessed for unauthorized purposes; or

- Records of personal health information have been copied, modified or disposed of in an unauthorized manner.

- Violation or imminent threat of violation of information security policies, standards, procedures or practices; or

- Information security event that may compromise operations or threaten the security of records of personal health information or related business process.
Additional examples

The following are additional examples of a privacy breach or security incident:

- Inappropriate access of personal health information
- Modification to your own or family members’ personal health information
- Inappropriate handling of printouts containing personal health information
- Misdirected printing of personal health information
- Sharing of login and password information
- Discussing personal health information with unauthorized individuals
- Theft or loss of personal health information
- Virus or malware infection; ransomware

• Viewing personal health information for a reason other than health care
  • About yourself
  • About your children, partners, spouses, friends and family
  • Of neighbours, public figures, exes, in-laws, etc. because you are curious (“snooping”)
• Searching personal health information for educational purposes as part of a research and/or teaching hospital using the ConnectingOntario viewer.

Left behind in a coffee shop or other public space.
Wrongly disposed of in a recycling bin, rather than securely shredded.

Printing to the wrong printer resulting in documents being viewed by unauthorized persons or being lost.

Colleague uses your account to quickly view an individual because you are already logged in.

Colleagues who are not providing or assisting in provision of health care.
Family or friends after work.
After employment ends or you retire.
### Personal Health Information Do’s and Don’ts

**Do....**
- Only view for individuals to whom you are providing health care.
- Only view information subject to a consent directive override for the purpose for which it was overridden and for the time required.
  - For example, do not print personal health information for later use. It can only be used at that time, for that purpose.
- Only share with those in an individual’s circle of care.
- Change your password if you suspect it may have been compromised and notify your Privacy Officer, Security Officer or eHealth Ontario as applicable.
- Create a strong and hard-to-guess password by following conventional guidelines and keep your password a secret.

**Don’t....**
- Discuss or view information in public places where others may hear or see.
- Take a picture of information displayed on an electronic health record screen.
- Send information from or to any unsecure email accounts, such as Hotmail and Gmail, including your own.
- Include your user name or password in any automated single sign-on process unless approved by eHealth Ontario.
- Leave your login open and unattended.

- Must meet the required number and type of characters for that application or system.
- Never create a password that includes your staff ID number, 3 consecutive letters, an easily recognized pattern, or easily obtained personal information about yourself.
- Create a unique password for access to health information and other systems, which is different from your personal email banking passwords or PIN.
- Commit your password to memory- only record it if it can be stored securely.
- Recommend using phrases when creating your password (e.g. ILOv2EatPizza).
# Personal Health Information Do’s and Don’ts

<table>
<thead>
<tr>
<th>Do....</th>
<th>Don’t....</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Always change an initial or temporary password provided to you on first use.</td>
<td>• Leave a computing device in public places or in your car in plain view. Take it with you or lock it in your trunk.</td>
</tr>
<tr>
<td>• Only use approved devices or processes to access either remotely or locally.</td>
<td>• Disable, bypass or override any information security controls including virus protection.</td>
</tr>
<tr>
<td>• Only use your own login and protect it. You are accountable for any actions tracked to your login account.</td>
<td>• Attempt to exploit a real or suspected security weakness.</td>
</tr>
<tr>
<td>• Immediately report all suspected or actual privacy breaches or security incidents following your organization’s or practice’s policies and procedures.</td>
<td>• Do anything that will interfere with the system’s normal operations or the integrity of the information processed by the system.</td>
</tr>
<tr>
<td>• Support your Privacy Officer or eHealth Ontario when they conduct an audit of access to personal health information.</td>
<td></td>
</tr>
<tr>
<td>• Use encrypted devices.</td>
<td></td>
</tr>
<tr>
<td>• Only store the minimum amount of personal health information necessary (if your organization or practice permits downloads to a portable device).</td>
<td></td>
</tr>
</tbody>
</table>

## Know Your Role in a Privacy Breach or Information Security Incident

In the event of an actual or suspected privacy breach or information security incident, you need to:

1. **Report:** If you suspect a privacy breach or information security incident has occurred at TOH or in relation to eHealth Ontario’s shared electronic health record systems, report it immediately to your manager and TOH or UOHI’s Information and Privacy Office.

2. **Contain:** Take reasonable and safe measures to contain the privacy breach or information security incident. For example, if you suspect someone has used your login, change your password. Do not destroy evidence (for example, a misdirected fax). It will assist in the investigation and may be needed to contact individuals.

3. **Cooperate:** Be prepared to cooperate in an investigation as required and to assist in any remediation activities.
2.20

Privacy Breach or Information Security Incident:
Corrective Actions

Any staff who breaches patient privacy, or violates TOH’s Privacy and Information Security Policies and Acknowledgement of Confidentiality are subject to the corrective actions below depending on the type of breach.

<table>
<thead>
<tr>
<th>Intentional</th>
<th>Intentional</th>
<th>Intentional</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-malicious breach</td>
<td>malicious breach</td>
<td>accidental breach</td>
</tr>
</tbody>
</table>

Click on each tab

Note: If you breach privacy when accessing eHealth Ontario’s shared electronic health record systems, these sanctions may also apply.

### Intentional non-malicious breach

**Examples:**
Looking up a co-worker’s chart because you are worried about their health

**Possible sanctions:**

- Suspension or Termination
- Report to professional and regulatory college
- Report to Information and Privacy Commissioner
- Fines/Prosecution

### Intentional malicious breach

**Examples:**
Snooping on your family, friends, colleagues for personal gain or to cause harm to another

**Possible Sanctions:**

- Termination
- Report to professional and regulatory colleges
- Report to Information and Privacy Commissioner
- Fines/Prosecution
Examples:
caused by carelessness, lack of knowledge or human error - such as emailing a fax or document to the wrong person

Possible Sanctions:
• Counselling Letter
• Possible report to professional and regulatory college
• Report to Information and Privacy Commissioner
• Fines/Prosecution

Notification to Patients When a Breach Happens

Patients will be informed if their personal health information has been lost, stolen or accessed for unauthorized purposes.

This may include the name of the staff or individual who caused the privacy breach or security incident.
Legitimate TOH purposes include:

i. Delivery of patient care;
ii. Hospital administration;
iii. Support for and promotion of education and research that has been approved by the Research Ethics Board;
iv. Quality assurance;
v. Documentation of patterns of illness to support prevention programs and early disease detection;
vi. Fundraising, provided express consent has been obtained or with implied consent where the information consists only of the patient’s name and contact information;
vii. Meeting TOH’s legal and regulatory requirements
TOH and eHealth Ontario: Differences

Staff may collect PHI to the extent necessary for other legitimate purposes prescribed by TOH.
The purpose for collection must be identified by the user of PHI at the time of collection.

Be Aware that in eHealth Ontario’s shared electronic health record systems, collecting/using/disclosing PHI for any purpose other than providing direct care (e.g. research, training) will constitute a privacy breach.

Patient Rights Relating to their Personal Health Information

By law, patients or their Substitute Decision-Makers have the right to:

- Refuse, withdraw or place restrictions on consenting to the collection/use/disclosure of their personal health information where the law permits
- Access and correct their personal health information
- Make privacy and security inquiries and complaints
Consent:
Under the law, health care organizations may rely on implied or express consent to view personal health information to provide individuals with care. A health care provider who receives a patient’s personal health information from
• the patient
• the substitute decision-maker
• or another health care provider
for the purpose of providing or assisting in providing health care to the patient may assume that he or she has the patient’s implied consent to
• collect
• use
• and disclose
the information for health care purposes, unless the health care provider is aware that the patient has expressly withheld or withdrawn the consent (e.g. by placing a privacy warning flag or consent directive).

Patient Rights: Withdrawal of Consent
I don’t want people to see my file. How do I make sure this happens?
If a patient or their Substitute Decision-Maker asks to:
• block their personal health information at TOH or UOHI or in eHealth Ontario’s shared electronic health record systems
or
• place restrictions on the record
...refer to Appendix A of TOH’s “Patient Privacy Policy” for details on who to contact

Individuals can place different types of consent directives on their personal health record. Please refer to Appendix A of TOH’s “Patient Privacy Policy” for details on who to contact. Contact the Information and Privacy Office for more information.
OHRI and UOHI:
Follow TOH’s policies and procedures

eHealth Ontario:
eHealth Ontario’s privacy and security policies for its shared electronic health record systems can be found online at: http://www.ehealthontario.on.ca/en/initiatives/resources

In addition to these 3 circumstances, TOH permits limited exceptions for going beyond a blocked record. Please contact the Information and Privacy Office for more information.

When can you view blocked PHI?

There are only 3 circumstances in which you are permitted to view blocked personal health information in TOH’s electronic health record systems and/or eHealth Ontario’s shared electronic health record systems:

1. When you have consent
2. Preventing harm to the patient
3. Preventing harm to others

In all 3 cases be sure to document the reason in the health chart for audit purposes.

Warning for OLIS Users:
In the Ontario Laboratory Information System (OLIS) an override to prevent harm is not permitted; rather, a block may only be overridden in OLIS with express consent by the patient or Substitute Decision Maker.
1st circumstance
When you have:

• verbal or written consent from an individual or substitute decision-maker

   and

• the personal health information is required for health care purposes

Get verbal or written consent by informing the individual:

• Of the purpose for viewing personal health information;
• That they have the right to give or withhold consent;
• Of the length of time the information will be viewable and who it may be viewed by; and
• That personal health information can only be viewed for the reason the consent directive was overridden.

2nd Circumstance
To prevent harm to the individual and you are not able to obtain consent in a timely manner.

3rd Circumstance
To prevent harm to another individual or group of individuals.
When a consent directive is overridden, the personal health information is only available:

**In ConnectingOntario**: To the user that initiated the override up to 11:59 pm the day that the override was initiated.

**In the Diagnostic Imaging Common Service (DI-CS), Ontario Laboratories Information System (OLIS)**: For 4 hours by any user within the organization.
Under the law, individuals also have the right to file a complaint to the Office of the Information and Privacy Commissioner of Ontario.

Privacy and Information Security Protocols: E-mail

**Internal emails**
Personal health information (PHI) can only be sent internally and to secure e-mail users (i.e. @toh.ca, @ohri.ca, @ottawaheart.ca and ONE Mail accounts) where the recipient has a “need to know” the information and precautions are used.

**Remember to:**
- Only use your TOH email for TOH business
- Do not auto-forward your TOH email to another account (e.g. Gmail™, Yahoo™, Hotmail™)
- Do not open attachments unless you know who it is coming from
- Recognize and report “Phishing Attacks” (e.g. email asking for your password)
e-mail Precautions

1. Use “Private” and “Confidential” flags to alert the recipient that the message contains PHI.

   a) Adding privacy or confidentiality flags to an e-mail (Outlook 2010): on the message tab find the Tags section and click the arrow to see more options.

   - On the Properties window, you'll find the Confidential and Private flag options under “Sensitivity” options.

   - When you select one of these the recipient will see an information icon with a request.
2. *Do not include PHI in the subject*

![Image showing email subject field with PHI]

3. *Look at the “To” fields before sending the message.*
   *Make sure you are sending it to the correct people.*

![Image showing email address field]

4. *Make sure when using a “Distribution List” or “Contact Group” that you are sending it to the correct people.*
Privacy and Information Security Protocols:

**E-mail**

**External emails**

E-mails sent **externally** should not transmit PHI except in the following special circumstances:
- Where no other means of communications are deemed feasible; and,
- Where messages are required for emergency health purposes between care providers

If an e-mail message must be sent externally for emergency health purposes, you must use the same precautions as used for internal e-mails and only send de-identified PHI.

If you can’t de-identify the PHI then you should:
- attach it in a document; and,
- encrypt the information and call the individual with the password to decrypt (do not sent the password by email!)

**Adequate alternatives include by fax, courier, mail or by accessing the information directly on an electronic health record.**

**De-identification** is a process to make legally protected personal health information unidentifiable. Potential identifiers include patient name, medical record numbers, and other health data content that could be used to identify an individual.

**Encryption** is a process which is applied to data, and alters it to make it unreadable except by someone who knows how to decrypt it. This makes it very hard for unauthorized people to view the data.
Privacy and Information Security Protocols: The Internet

When using the Internet, it is important to remember that the Internet is not private.

For safe Internet use:
- Do not let web browsers remember your passwords
- Do not upload sensitive, hospital-related information, including PHI, to third party, cloud-based file services such as Dropbox™, Google Drive™, Google Docs™, etc.
- Do not store information on your PC desktop or C:drive, or on a mobile device
- Use hospital-approved applications, such as Microsoft Office365™ and Sharepoint™, appropriately and for authorized purposes

Privacy and Information Security Protocols: Social Media

Personal health information (PHI) should never be discussed on social media, such as Facebook®, Twitter®, etc.

Without disclosing the patient’s name, if you provide a patient’s
- age
- condition
- where you work in the hospital

... that individual could be identified and you have breached their privacy!
Privacy and Information Security Protocols: Photos and Videos

Do not snap a picture or shoot a video of
- patients
- or
- personal health information displayed on any of TOH or eHealth Ontario’s shared electronic health record systems

Photography and videography are only permitted for **legitimate purposes and with patient consent**

**Legitimate purposes?**
Please refer to TOH’s Patient Privacy Policy, Media Relations Policy, and/or associated policies for permitted purposes of photography and videography.
Privacy and Information Security Protocols: Mobile Devices and Laptops

If you have a mobile device that is connected to TOH, you are accountable for all activity using TOH resources (email, network, applications).

To protect and secure laptops, ensure they are

- encrypted
- locked up
- password protected

And data is securely backed up

Remember!
Do not store personal health information on mobile devices or laptops for longer than necessary.

If any of the above devices are lost or stolen, immediately report it to the HelpDesk (613-761-HELP)!

⚠️ Remember!

Never share your mobile device with family, friends or co-workers. Never share your passwords and protect the device from loss or theft.

❓ Encrypted with full disk encryption.
This means the entire computer is encrypted, not just the data.

❓ Locked up in the trunk of your car.
Locked in your desk or on top with a cable.

❓ Use a strong and complex PIN # (e.g. do not use “1234”) and password protected screen savers.
Privacy and Information Security Protocols: USB Flash Drives

For safe and secure use of USB Keys follow the Stop, Think, Protect model

STOP... Ask yourself:
- Do I really need to store any personal health information on this device?

THINK... Consider the alternatives:
- Would de-identified or encoded information serve the same purpose?
- Could you access the information remotely through a secure connection or virtual private network (VPN) instead?

PROTECT... If you must store personal health information on mobile devices make sure:
- It is strongly encrypted
- It is protected with strong passwords
- Be sure to regularly scan your USB for viruses

Remember!
Do not store personal health information on a USB for longer than necessary.
If your USB is lost or stolen, immediately report it to the HelpDesk (613-761-HELP)!

Your Information and Privacy Office (IPO)

The Information and Privacy Office (IPO) at TOH and UOHI wants to protect the careers of staff by informing them of their privacy obligations and ensure the trust of our patients by safeguarding and respecting the confidentiality of their personal health information.

The three objectives of the IPO are to achieve high visibility, high impact and high compliance around privacy and security matters at the Hospital.

To learn more about what can be done to protect our patients’ personal health information please visit the Privacy Webpage located on myHospital and review privacy and security policies.

Click on the organization you work for below to obtain the contact information when reporting any privacy or security related breach, incident, inquiry or complaint.

Privacy and Security at TOH and OHRI
Privacy at UOHI
Contacting the Information and Privacy Office at TOH & OHRI

For privacy inquiries:
Phone: 613-739-6668
Fax: 613-761-4740
Email: infoprivacyoffice@toh.ca

For information security inquiries:
Phone: 613-798-5555 x71444
Email: ISSecurityRequests@toh.ca

Contacting the Information and Privacy Office - UOHI

For privacy inquiries:
Phone: 613-696-7000 ext 13575
Email: JLajeunesse@ottawaheart.ca

For information security inquiries:
Phone: 613-696-7000 ext 13457
Email: HPika@ottawaheart.ca
CONFIDENTIALITY AGREEMENT:

At The Ottawa Hospital (TOH or the Hospital) and our affiliated institutions, we are committed to protecting the confidentiality and security of all personal health information (PHI) of our patients, confidential information (CI) and personal information (PI) with which we are entrusted.

The PHI and PI over which TOH has stewardship is subject to the provisions of:
- the Personal Health Information Protection Act, 2004 (PHIPA)
- the Freedom of Information and Protection of Privacy Act (FIPPA) as well as
- TOH policies and procedures

CONFIDENTIALITY AGREEMENT:

PHI, PI and CI

Personal health information (PHI)
For the purposes of this Agreement, PHI has the same meaning as defined in section 4 of PHIPA, and generally refers to any identifying information about an individual’s health care history, such as medical history, details of visits to a doctor, test results or health number.

Personal information (PI)
PI has the same meaning as defined in section 2 of FIPPA, and refers to recorded information about an individual. This may include the individual’s name, address, sex, age, education, medical or employment history - and any other information about the individual.

Confidential information (CI)
CI means any non-public information of TOH, in any form, which considering all the circumstances ought reasonably to be understood as confidential. CI includes but is not limited to information related to applications, research, products, inventions, processes, designs, business plans, services, customers, marketing, finances or information gained as a result of business relationships or discussions with TOH’s personnel. CI also includes any information derived from or incorporating the foregoing information.
The TOH Confidentiality Agreement must be completed by all employees, students, contractors, physicians, volunteers, researchers, and other affiliates.

Thank you for your commitment to protecting and respecting the Personal Health Information of our patients.