2016 Privacy and Information Security

Course Objectives

By the end of this training, you will understand your

1. privacy and security obligations as a staff of TOH, OHRI, and UOHI

Am I considered Staff of TOH?

2. privacy and security obligati ons related to patients and as a user of TOH's electronic health record systems. This includes, but is not limited to:
    - OACIS,
    - PACS,
    - eHealth Ontario's shared electronic health record systems (e.g. Ontario Laboratory Information System (OLIS), Diagnostic Imaging Common Services (DI-CS), Connecting Ontario/cNEO)

Important!

There are differences in how eHealth Ontario's shared electronic health record systems operate - those will be identified where applicable.

Am I considered Staff of TOH?

Staff includes all permanent or temporary, full-time, part-time, casual or contract employees, trainees and volunteers, including but not limited to physicians, residents, interns, researchers and students

Why Protect Privacy?

It's the law!

It's your professional obligation!

It's the *right thing* to do!

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

- Your position at TOH, career and reputation
- Review and discipline by professional and regulatory colleges
- $50,000 in personal fines
- A civil lawsuit and/or prosecution

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 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)** is the law that protects the privacy of an individual and the confidentiality of an individual's personal health information.

What it 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.

Click to see examples of PHI

Click to see examples of PHI

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, we use security safeguards to help protect personal health information against

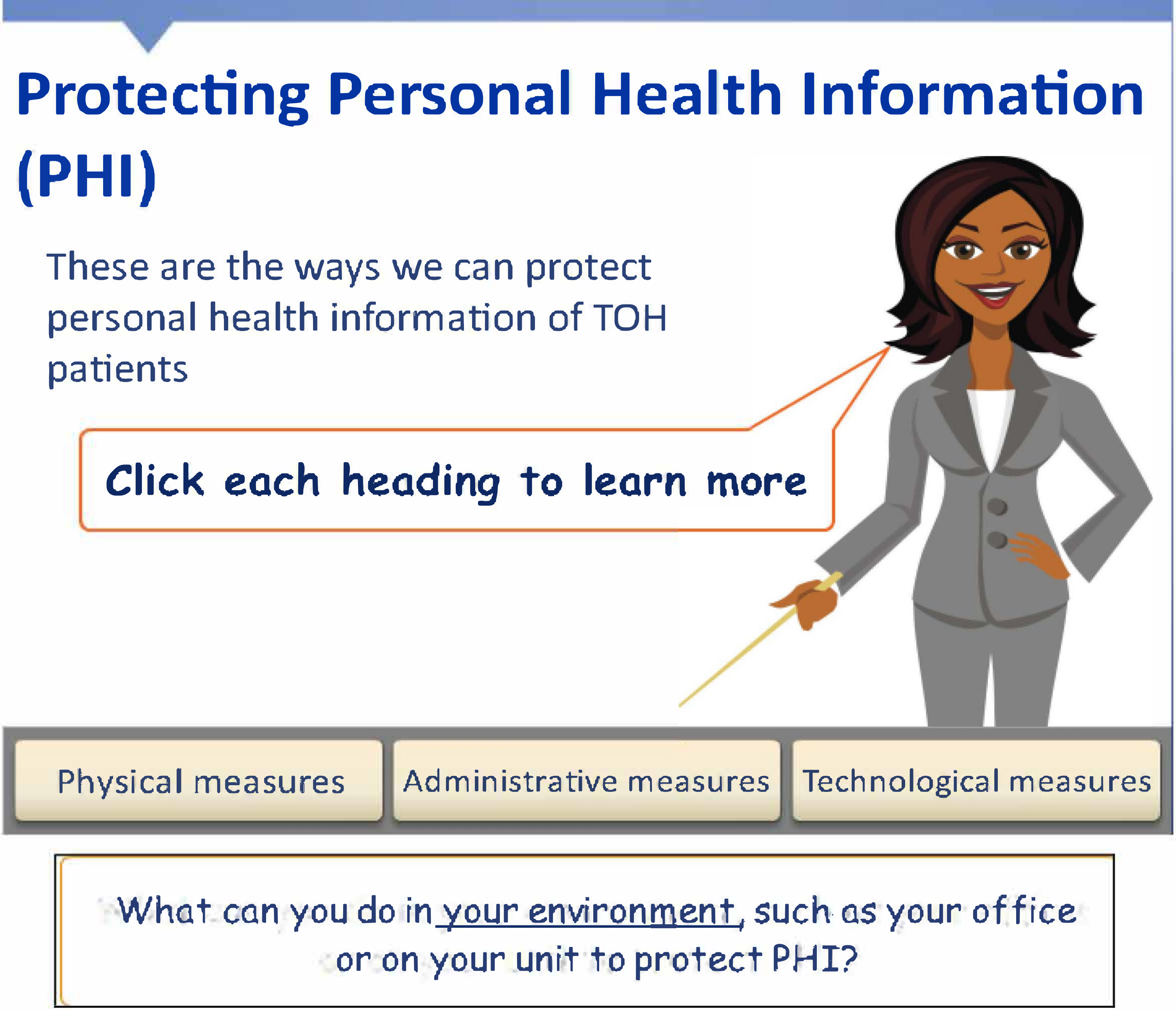
- loss or theft
- unauthorized access , disclosure, copying, use or modification

Note:

eHealth Ontario

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
http://www.ehealthontario.on.ca/images/uploads/regional_partners/ConnectingOntario_health_care_provider_guide-en.pdf



Protecting Personal Health Information (PHI)

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

Click each heading to learn more

What can you do in your environment, such as your office or on your unit to protect PHI?

Physical Measures

- 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

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.

Protecting Personal Health Information (continued)

What processes already exist in your workplace or can be put in place by you to protect personal health information (PHI)?

Administrative Measures

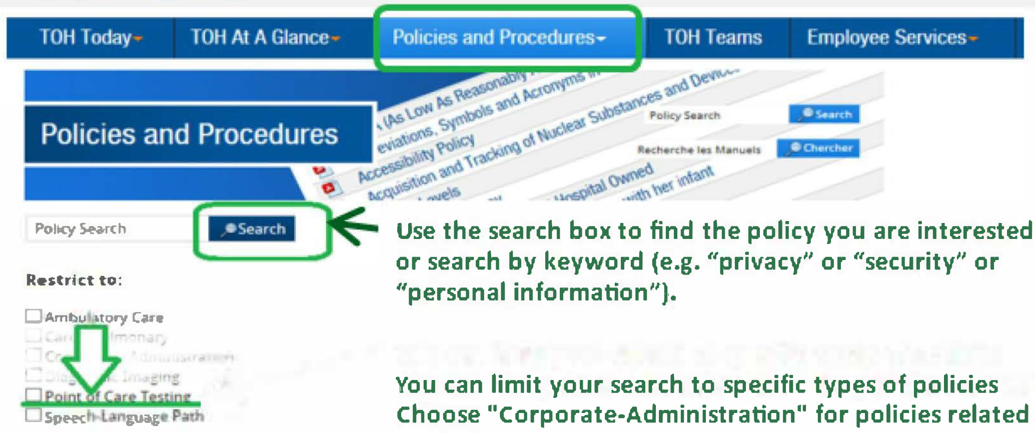
- Confirmation of identity before providing access to PHI
- Limiting access to personal health information to a "need to know basis"
- Requirements to sign agreements to protect PHI
- Awareness and Training
- Policies and Procedures

Click here to learn where to find policies and procedures

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.



Use the search box to find the policy you are interested in, or search by keyword (e.g. "privacy" or "security" or "personal information").

You can limit your search to specific types of policies Choose "Corporate-Administration" for policies related to Privacy

Click the icon for information on eHealth Ontario, OHRI or UOHI Policy/Procedure 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

Protecting Personal Health Information (continued)

What technical measures (or safeguards) are available to protect personal health information?

Technical Measures

- Use of firewalls and encryption
- Strong password requirements and a rule that individuals do not share or write down those passwords ①
- 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 ②
- Auditing of all systems to detect unauthorized access ③

Passwords

① 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

② If you need to leave your computer you must either:

- Lock the screen by pressing 4

  Ctrl - Alt - Del

Auditing

③ 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

Remember:

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

Understanding Privacy Breaches and Security Incidents

A privacy breach and/or security incident is the unauthorized access, collection, use or disclosure of Personal Health Information (PHI)

It may be:

Intentional: purposely accessing the PHI of your neighbour when you do not require such information to do your job

Inadvertent: accidently sending a patient's medical report to the wrong fax number or discussing personal health information in public places

A privacy breach or security incident can also include:

- **Failure to protect PHI**
- **ANY lost or stolen PHI**
- **Contravention of any provision** of the *Personal Health Information Protection Act*, TOH privacy and security policies, and privacy and security obligations in agreements

Failure to protect PHI

sharing passwords, leaving health records unattended or inappropriately disposing of PHI

Contravention of any provision

Examples
(e.g. TOH's Acknowledgement of Confidentiality, eHealth Ontario's End User Agreement, etc.)

Know Your Role in a Privacy Breach or Security Incident

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

1. Report:	If you suspect a privacy breach or 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 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

Privacy Breach or Security Incident Sanctions

Any staff who breaches patient privacy, or violates TOH's Privacy and Security Policies and Acknowledgement of Confidentiality are subject to the sanctions below depending on the **type** of breach

Intentional non-malicious breach	**Intentional** malicious breach	**Inadvertent** accidental breach

Click on each tab

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

Privacy Breach or Security Incident Sanctions (continued)

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

Inadvertent
accidental breach

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

Understanding similarities and differences:

TOH and eHealth Ontario's electronic health record systems

The Ottawa Hospital | L'Hôpital d'Ottawa

As a user of TOH's electronic health record systems (e.g. OACIS) you may collect, use, and disclose personal health information (PHI)

eHealth Ontario

As a user of eHealth Ontario's shared electronic health record systems, **you may only** collect, use, and disclose personal health information (PHI)

when providing or assisting in health care ('circle of care')

What are "other" legitimate purposes?

Understanding similarities and differences (continued)

What are “other” legitimate purposes?

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

The Ottawa Hospital L'Hôpital d'Ottawa

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.

What are "other" legitimate purposes?

eHealth Ontario

!

__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

Click to learn more about consent

Patient Rights Relating to their Personal Health Information (continued)

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

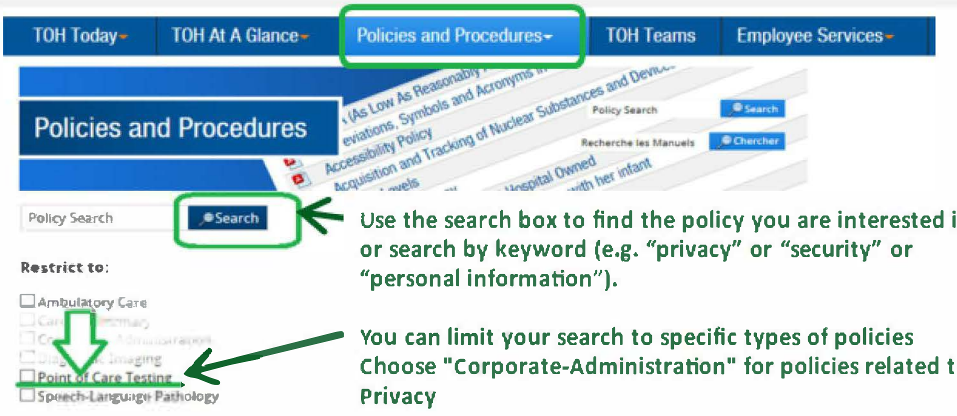
- place restrictions on the record

…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.

Click here to learn where to find policies and procedures

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



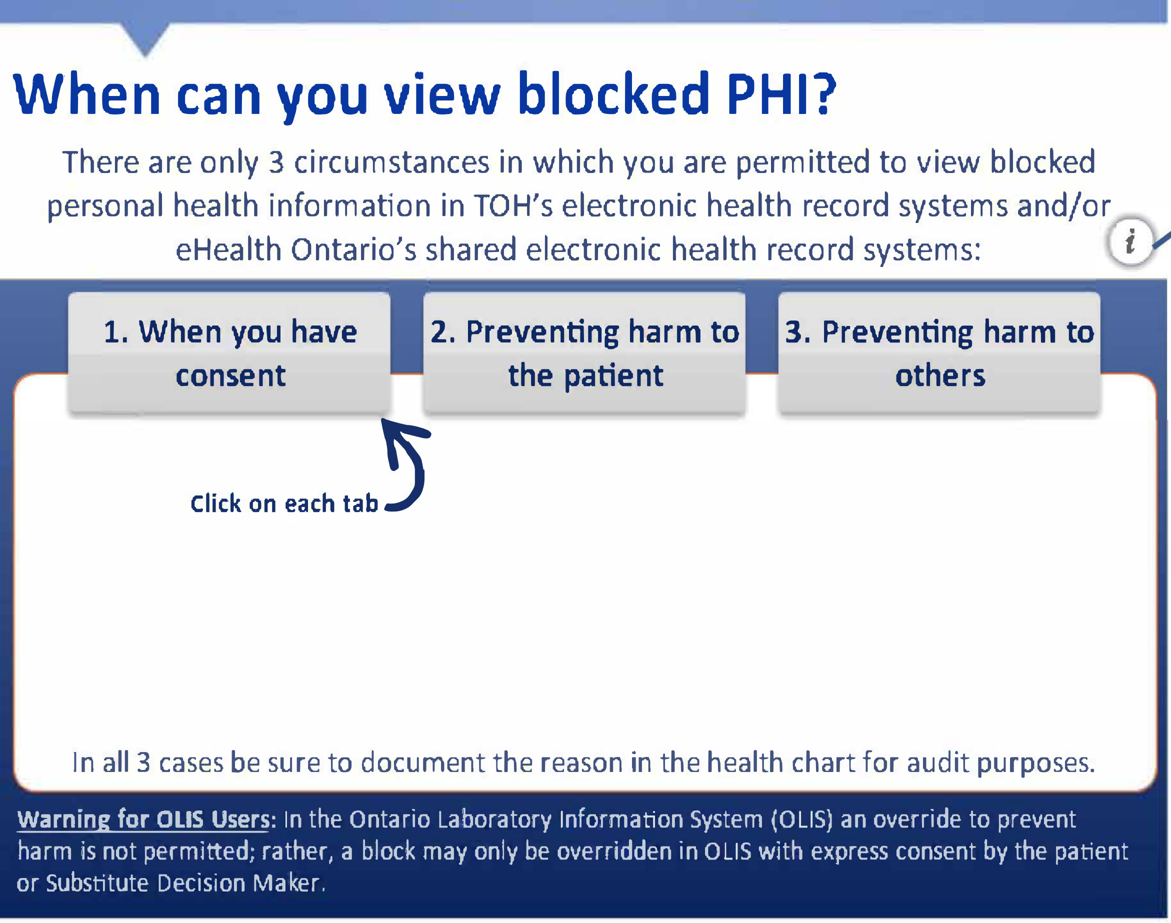
Use the search box to find the policy you are interested in, or search by keyword (e.g. “privacy” or “security” or “personal information”).

You can limit your search to specific types of policies Choose "Corporate-Administration" for policies related to Privacy

Click the icon for information on eHealth Ontario, OHRI or UOHI Policy/Procedure information…

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



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
Click on each tab

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.

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.

1. When you have consent

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

2. Preventing harm to the patient

2nd Circumstance

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

3. Preventing harm to others

3rd Circumstance

To prevent harm to another individual or group of individuals

If you have viewed a blocked record for one of the three accepted reasons …

- Only view the information for the documented purpose for which you overrode the blocked record
- Be prepared to explain the reason for the override if requested by the patient to whom the information relates or by the Information and Privacy Office
- The Information and Privacy Office may notify the individual when his or her blocked personal health information has been viewed (including details on who accessed the record and the reason for the override)
- Keep in mind that eHealth Ontario's shared electronic health record systems limits the amount of time a clinician can view a blocked record

Remember! TOH investigates all overrides of blocked records to ensure the access was appropriate and authorized.

Patient Rights:
Access & Correction, Questions & Complaints

If a patient (or Substitute Decision-Maker) wishes to obtain a copy or make a correction to their personal health information, direct them to Health Records.

Please refer to TOH's Patient Privacy Policy for more information

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 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** <u>and</u> ONE Mail accounts) where the recipient has a "need to know" the information and precautions are used.

Remember to:

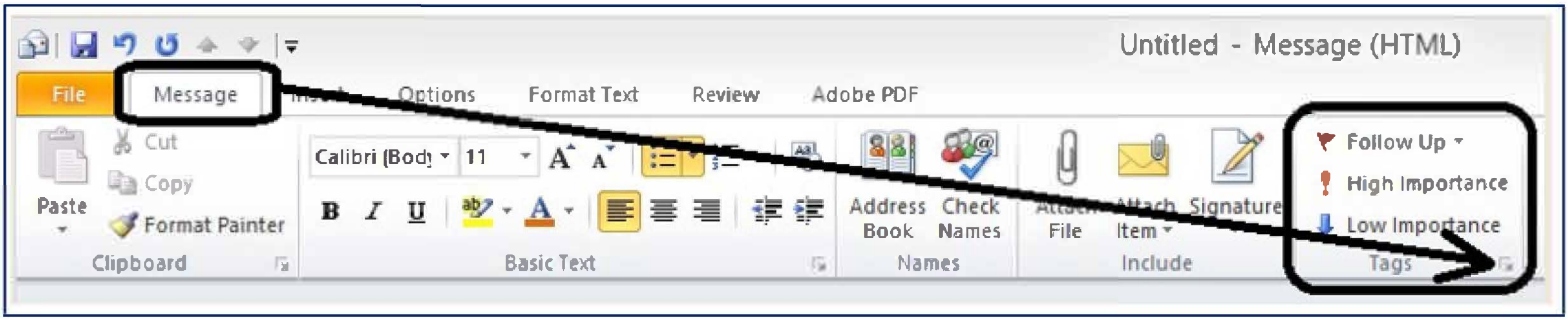
- Only use your TOH email for TOH business
- Do not auto-forward your TOH email to another account (e.g. gmail, Yahoo, hotmail)
- Do not open attachments unless you know who it is coming from
- Recognize and report "Phishing Attacks" (e.g. email asking for your password)

Click here → **email security tips**

e-mail Precautions

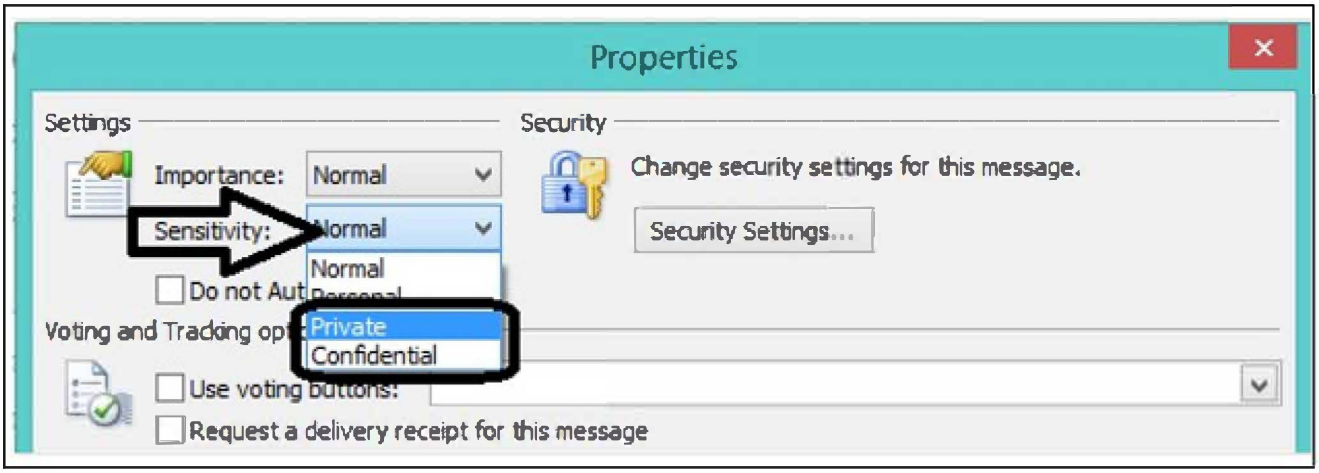
① *Use "Private" and "Confidential" flags to alert the recipient that the message contains PHI.*

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



Privacy and Security Protocols
Email – Internal emails (continued)

b) ***On the Properties window, you'll find the Confidential and Private flag options under "Sensitivity" options.***



Importance: Normal

Sensitivity: Normal

□ Do not Aut

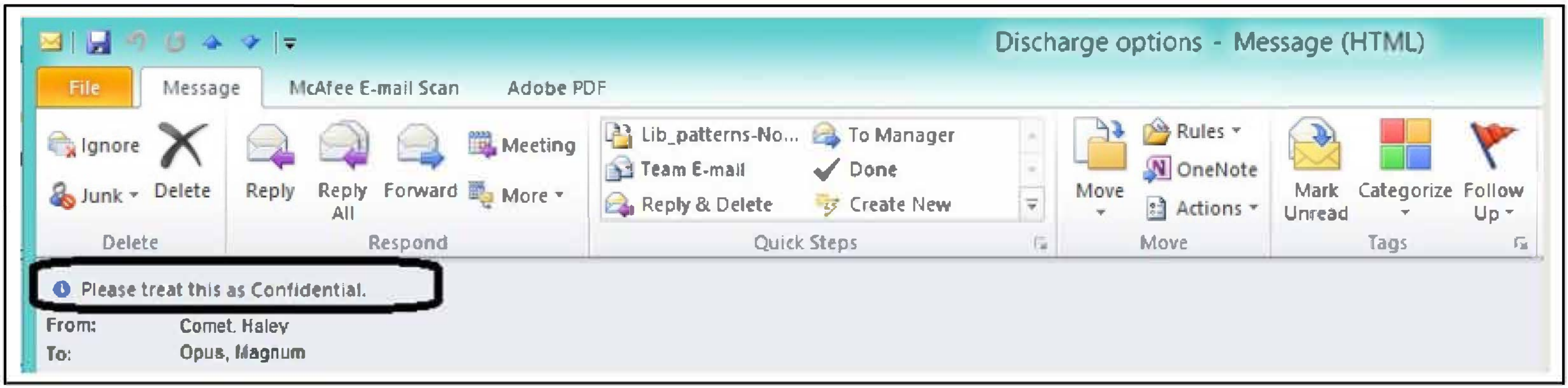
Change security settings for this message.

Voting and Tracking opt

□ Use voting buttons:

□ Request a delivery receipt for this message

c) ***When you select one of these the recipient will see an information icon with a request.***



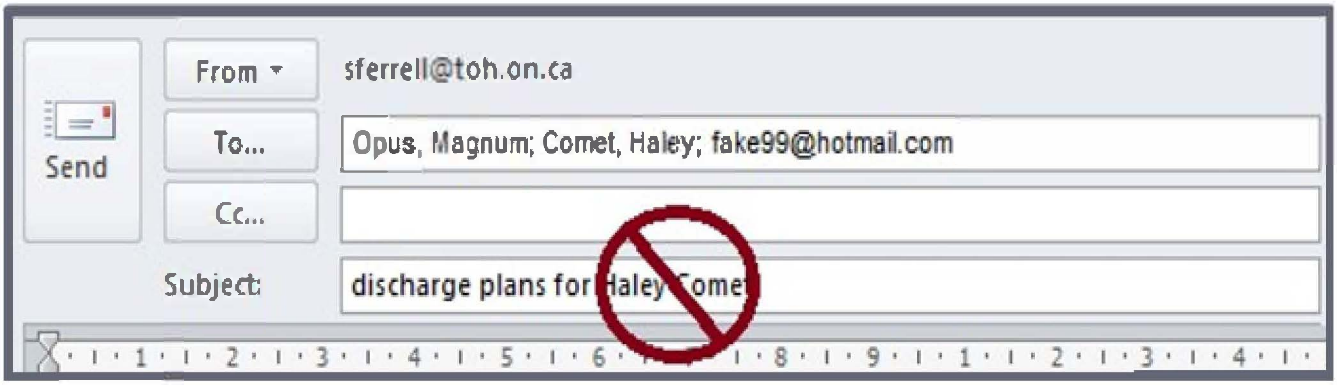
Please treat this as Confidential.

From: Comet, Haley

To: Opus, Magnum

Privacy and Security Protocols
Email – Internal emails (continued)

② *Do not include PHI in the subject*



From: sferrell@toh.on.ca

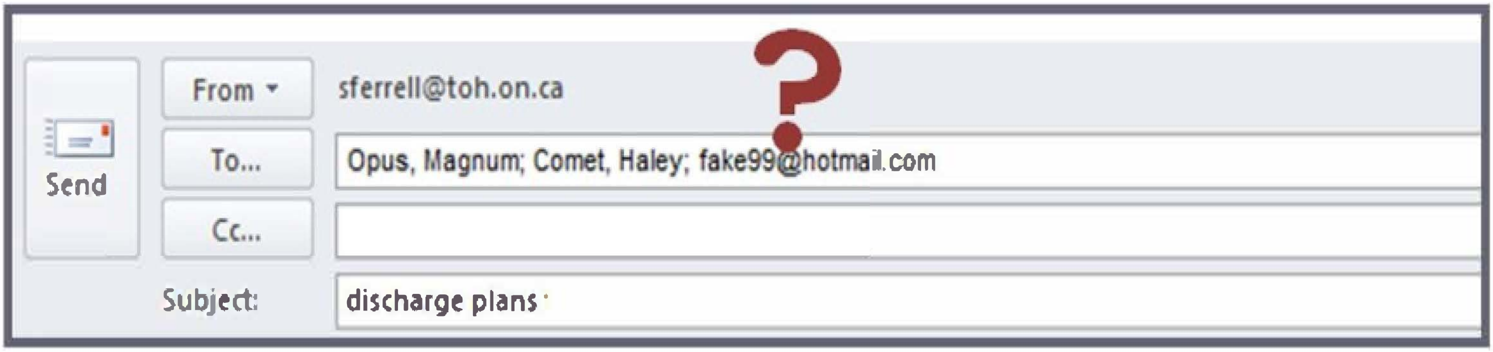
To...: Opus, Magnum; Comet, Haley; fake99@hotmail.com

Cc...:

Subject: discharge plans for Haley Comet

③ *Look at the "To" fields before sending the message.*

Make sure you are sending it to the correct people.



From: sferrell@toh.on.ca

To...: Opus, Magnum; Comet, Haley; fake99@hotmail.com

Cc...:

Subject: discharge plans

④ *Make sure when using a "Distribution List" or "Contact Group" that you are sending it to the correct people.*

Privacy and 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 adequate; 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 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 PHI to Dropbox®, Google® docs
- Do not store info on your desktop or C:\Drive

Privacy and 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 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 **<u>legitimate purposes and with patient consent</u>**

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 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 & 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.

The Ottawa Hospital | L'Hôpital d'Ottawa

The Ottawa Hospital | L'Hôpital d'Ottawa
Research Institute | Institut de recherche

University of Ottawa Heart Institute
Institut de cardiologie de l'Université d'Ottawa

Privacy and Security at TOH and OHRI

Privacy at UOHI

Your Information and Privacy Office (continued)

Privacy and Security at TOH and OHRI

Contacting the Information and Privacy Office at TOH & OHRI

For privacy inquiries:

Phone: 613-739-6668 / Fax: 613-761-4740 / Email: privacy@toh.ca

For security inquiries:

Phone: 613-798-5555 x71444 / Email: jelemonde@toh.ca

Privacy at UOHI

Contacting the Information and Privacy Office - UOHI

For privacy inquiries:

Phone: 613-798-5555 x13575 / Email: JLajeunesse@ottawaheart.ca

For security inquiries:

Phone: 613-798-5555 x13457 / 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.

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