Privacy and Security Training at Trillium Health Partners

Trillium Health Partners
Better Together

Privacy and Security learning module

There are 4 parts to this training:

Part 1 is core privacy content
Part 2 is research security content
Part 3 is core security content
Part 4 is for all users of <u>ConnectingGTA (cGTA), REACH and other shared systems</u>

<u>You must review all slides and confirm you have read and understand this material before accessing cGTA.</u>

Objectives

By the end of this course participants will understand:

- PHIPA and Personal Health Information
- How to report a Breach of Privacy
- Key Concepts for computer security
- Good Security Practices
- Restrictions on use and disclosure specific to cGTA and other shared systems
- Where to find THP Policies and Procedures on Privacy and Security

Objectives

Keeping Personal Health Information private is…

✓an individual's right
✓a legal requirement,
✓a research standard,
✓a contractual commitment, and
✓a professional ethical obligation.

Privacy protection is critical to maintaining strong relationships with patients, who trust that their care providers will use the information to make accurate diagnoses and plan effective treatments.

This training course includes:

- requirements for using **internal THP electronic systems**, which only contain information about THP patients; AND

- Specific privacy and security guidance for users of **shared electronic systems** (such as **ConnectingGTA (cGTA), REACH, PRO, DI-Repositories and others**), which contain information about patients from different healthcare organizations.

Privacy Training

Part 1:

Core Privacy Training

Privacy Training - PHIPA

Ontario's ***Personal Health Information Protection Act, 2004*** ("PHIPA") defines how **personal health information** ("PHI") must be handled (collected, used and disclosed) by hospitals and other healthcare providers in Ontario (health information custodians ("HICs")).

PHIPA:

- Builds on older laws like the *Public Hospitals Act* and the *Regulated Health Professions Act* to protect PHI.
- Balances a patient's right to privacy against the need to share information within the "circle of care" so that timely, high quality care may be delivered
- Requires healthcare providers to protect PHI and to share it only as required for: (1) provision of healthcare or (2) other purposes allowed under PHIPA, including health system planning and research
- Provides patients with a right to access and request correction of their own PHI.

Personal Health Information (PHI)

What is Personal Health Information ("PHI")?
PHI is one of the most highly sensitive types of information that can be collected about a person.

PHI is information that:
identifies a person (**OR** can be combined with other information to identify a person), and connects that person with information about their health status or their healthcare delivery at THP or other health facilities.

Personal Health Information (PHI)

PHI may be found throughout the hospital in many forms, including:

- on paper (e.g. charts, printouts, handwritten messages & notes)
- in electronic files (e.g. electronic charts, letters, spreadsheets, reporting forms, email, internal electronic systems, shared electronic systems)
- in or accompanying biological materials (e.g. tissue, blood, DNA)
- in conversations with research participants or researchers

PHI can include a MRN or HCN, health care history, family medical history, test results, and diagnostic images and, in addition to formal documentation written on paper or in an electronic record, it can include information you know.

Remember: You have access to PHI because you are an 'agent' of THP, as defined in PHIPA, and need the access for the work you do at THP with THP patients.

Breaches/Incidents

PHIPA, as well as hospital policy and some shared system policies, require that individuals must be notified if their PHI is:

- lost;
- stolen; or
- inappropriately accessed (including if PHI is sent to someone not authorized to receive it or seen by someone not authorized to see it).

These situations are called privacy incidents or “breaches”

Privacy Incidents/Breaches and suspected breaches **must be reported immediately by YOU** if you are an employee, physician, dentist, midwife, volunteer, student, instructor or any other person working at or on behalf of THP **to the THP Manager of Clerkship & Postgraduate Medical Education or THP’s Privacy Office**.

You may be required to support the investigation, containment, or remediation of a privacy or security breach.

This training module will provide tips on how to avoid breaches

How can you report an incident?

Inform THP's Privacy Office (privacy@trilliumhealthpartners.ca);

OR

Inform the Manager of Student Services (bryan.abankwah@thp.ca)

Personal Health Information (PHI)

With limited exceptions, patients have the right to **access** their PHI and to request **correction** of inaccurate information in their record. If a patient asks to see, copy or correct their record, you should consult hospital policy to find out whether to do the following:

- Review the chart in person with the patient
- Provide the patient with a routine copy of encounter results
- Refer the patient to a more appropriate clinician to assess whether additional support is needed (e.g. to request order results),
- Refer them to Health Information Management (a.k.a. “HIM” or “Health Records”), or
- Request assistance if unsure, of if the request relates to correction.

Move quickly! While PHIPA permits 30 days to fill or refuse non-urgent requests or to communicate the reasons for needing more time, internal deadlines may be much shorter.

Remember…

Ask your supervisor or the Health Information Management (HIM) Department (905-848-7580 x 2855) if you’re not sure what to do when asked to release PHI for any reason.

Staff are not allowed to directly access their own medical record using a THP system. Staff must follow the same procedure as any other patient and submit a request to HIM.

Stop Privacy Breaches

The following are some examples of privacy breaches

- Faxing PHI to the wrong fax number
- Discussing PHI in public areas, even if the patient is not named
- Searching for a friend or relative on a clinical system out of curiosity or concern
- Saving PHI onto an unencrypted USB drive

Privacy Tips

Care settings can be busy and noisy and patients usually understand that there may be limits to protecting their privacy in practice.

There are things you can do to improve privacy assurance on the job. For example:

- If a patient asks to speak with you privately,   do what you can to find a quiet place to talk, and talk in a low voice.
- Don't discuss confidential information in public areas of the hospital (e.g. elevators, food courts) or in the community (e.g. on public transportation, when shopping, at home).
- Don't handle a patient's PHI unless you have a 'need to know', either because you are caring for the patient directly or have administrative authority to access their record
- Follow hospital policies and procedures for the collection, use and disclosure of PHI.

Using and Disclosing PHI

To facilitate effective health care, health research and to manage the health care system, PHI must be shared among a number of different people and organizations.

Appropriate disclosure of PHI includes sharing information:

- among the patient's "circle of care"
- With "agents" of the HIC who perform services on the HIC's behalf, e.g. administrative support professional
- With other service providers, e.g. external I.T. service providers who have contracts with THP

Implied Consent

Unless the patient has told us not to do so, care providers can **assume the patient's implied consent** to use & disclose (release/share) PHI but only within the patient's 'circle of care' and only as long as the information will be used to provide healthcare to that person.

Who can be part of the 'circle of care'? Anyone who…

- Currently provides care to the patient
- Performs a diagnostic test or interprets the results for the patient
- Prepares a care plan for the patient
- Sets up referrals & gathers information to transfer the patient to another facility or clinician
- Receives referrals and makes decisions about whether to accept patients
- Prints charts, gets exam rooms ready or otherwise supports the provision of care
- Moves patients from one department to another in the hospital
- Faxes or emails patient's results to a patient
- Schedules appointments for patients
- Prepares or delivers meals to patients
- Assists patients in paying their bill
- Cleans a patient room

Such as…

- THP physicians, nurses, allied health professionals, radiologists, students, volunteers
- External care providers (e.g. family physician, referring MD, laboratory, rehabilitation facility, CCAC)
  if they will use the information to provide direct care.

How do you get implied consent?

Consent is implied when:

- The patient discloses PHI in the normal course of receiving care

- A HIC discloses PHI to another HIC for the purpose of providing health care to that patient

- EXCEPTION: A patient may withhold consent to use or disclose some or all of their PHI in our records or in shared systems. This is often called a “consent directive” or “lockbox and means that such information cannot be accessed/used/disclosed except in very rare circumstances (consult a manager). On electronic systems it will be clearly flagged to prevent accidental access and all accesses will be logged and reported to the patient.

Express Consent

Express (verbal or written) consent is required whenever disclosing PHI to persons who are not HICs or are not part of the patient's circle of care.

You NEED express patient or SDM consent to disclose to:

- Patients' lawyers, employers, insurers, friends, family, classmates, students or professors
- External HICs for purposes other than the direct care of that patient (e.g. quality assurance)
- The public (e.g. for presentations or publications)
- Special rules apply to use PHI for marketing/fundraising – consult the Privacy Office
- Police – except in special circumstances. Escalate ALL police requests for PHI to your manager/on-call leadership.

Substitute Decision Maker (SDM)

An SDM (if patient is not capable) can also provide consent as if they were the patient:

- Always confirm whether a Substitute Decision Maker is acting on behalf of a patient for decisions involving PHI.

- If an SDM is acting for a patient incapable of making a decision about their information, ask the SDM for consent

Obtaining express consent

Obtaining EXPRESS consent:

- Consent must:
  - (i) be given by the patient or patient's SDM;
  - (ii) be knowledgeable;
  - (iii) relate to the information; and
  - (iv) not be obtained through deception or coercion.

- Describe the impact of giving or withholding consent (e.g. who will see the PHI and for how long) and ask the patient (or SDM) if they consent to use or disclosure of their PHI

- Document the consent in the patient's chart or other authorized method

Disclosure

Remember to ask patients or SDMs for their consent before…

- Giving out detailed updates to family or friends of patients in the hospital
- Leaving a detailed voicemail for the patient or their SDM

THP may disclose three items of PHI about a patient IN the hospital UNLESS the patient or the SDM has requested confidential status.

1) the fact that individual is a patient in the hospital;
2) the individual's general health status (critical, poor, fair, stable); and
3) the patient's location in the hospital.

- If "confidential" status, patient's name will have a small "c" in front of it on Meditech and charts.
- If "confidential" status, DO NOT disclose ANY information, not even whether or not you know if the individual is or is not in the hospital. Say: "I have no information about that person".

PHI on internal systems

You may use PHI for non-care purposes ONLY if the PHI is in/from an internal THP electronic system (e.g. EPR) or paper record. Using an internal THP system, unless the circumstance requires express consent:

You may use PHI for teaching when you:

- Are in a recognized teaching program affiliated with the hospital
- Have approval from your manager or Chief of service
- You are part of the patients' care team

You may use PHI for quality control, risk management and program planning only when this is part of your job.

You may use PHI for research only with REB and institutional approval (http://thphub/education/research-operations/Pages/default.aspx)

PHI on shared systems

YOU MAY NOT ACCESS A SHARED SYSTEM (e.g. cGTA, REACH, PRO, DI-Repositories, etc.) **FOR TEACHING, QUALITY CONTROL, RISK MANAGEMENT, PROGRAM PLANNING OR RESEARCH!**

This would constitute a serious breach of contract

Use shared systems only for providing direct care to a patient

PHI and the Internet

Be careful online…

Unless the patient has provided their express consent which is documented in the chart:

- Do not post <u>any</u> PHI, including photos, videos or other recordings of patients on any internet site. (e.g. Facebook, Twitter, YouTube, blogs).

- Do not describe work situations online.
  - Patients may be recognizable even when common identifiers (e.g. patient names and hospital numbers) are removed.

- If accessing your hospital email via webmail, do not open or save attachments with PHI on a public, shared or personal computer.

Photographs

Taking photos, videos of patient or staff

- If taking a photo to support patient care (e.g., wound) explain to patients why a photo is being taken and what will happen with it (e.g., kept in the chart).
- If taking a photo to be used in public media, Public Affairs must be notified and the patient must provide their express consent in advance
- If taking photos for educational purposes, images must be de-identified
- Photos must not remain on portable devices and must be deleted from the device as soon as possible after being taken and after the photo has been copied elsewhere (if needed)
- You cannot take photos, videos or audio recording of clinicians or staff without their express consent
- Clinicians or staff must be asked by a patient or family member for their consent before a photo, video or taping is done by the patient or family member

.

Social Media

Social Media

- Social media cannot be used to convey PHI to patients or colleagues

Texting

- Texting PHI (including acknowledgments, appointment reminders, test results) is not permitted

How do I ensure a photo or video is de-identified?

- No identifying information should be visible in the picture
- The background of a photograph or video should be checked for PHI and nobody who has not consented to the image capture should appear
- Avoid personal identifiers e.g., face tattoos, etc. unless clinically necessary when capturing images
- If the location where a photo was taken is confidential, turn off the device's GPS feature before taking photos so that location information is not automatically captured in the photo's meta data.

Warning

Think First before you access or disclose PHI!

Accessing PHI for which you have no professional ‘need to know’ is termed ‘inappropriate access and **is a privacy breach under PHIPA and under THP’s Privacy Policy.** It is also a breach of your employment or other agreement with THP, and, if applicable, regulatory college practice standards.

This means you **must not** access any record of a patient for whom you either do not have a duty to care, or a duty to administer to the record in your role at THP, whether as employee, physician, volunteer, agent or other. Your access of any record should reflect only your “need to know”.

This includes not accessing records belonging to family, friends or colleagues whose care you are not involved with as an authorized agent of THP, refraining from discussing patient information in public areas, and refraining from bypassing hospital procedures to review your own health records.

Inappropriate Access to PHI

The consequences to you of engaging in inappropriate access to patient or other corporate confidential information may include:

- Loss of access to one or more information systems;
- Report to professional college, where applicable, loss of professional standing, college sanctions and regulatory fines;
- Disciplinary action up to and including termination of employment, termination of hospital privileges or hospital affiliation or termination of a contractual relationship; and
- You can be charged or sued in court.

Be Privacy Aware – **Think First before Accessing PHI!**

Summary of PHI

- Does not prevent the provision of care or sharing of PHI within the “circle of care”
- Builds on what you already know and do
- Confers certain rights to patients
- Promotes accountability for patient’s privacy
- Allows the HIC to use PHI for system planning and delivering health care services
- Frequently is the root cause of patient complaints

Golden Rules of Privacy

Think First: Do I NEED access to this PHI?

- Respect people's privacy and only access the records and information you need to perform your duties.

- Do not access information about your family, co-workers, or any patient not under your care or for whom you do not have a 'need-to-know.'

- "Viewing" PHI is logged and audited.

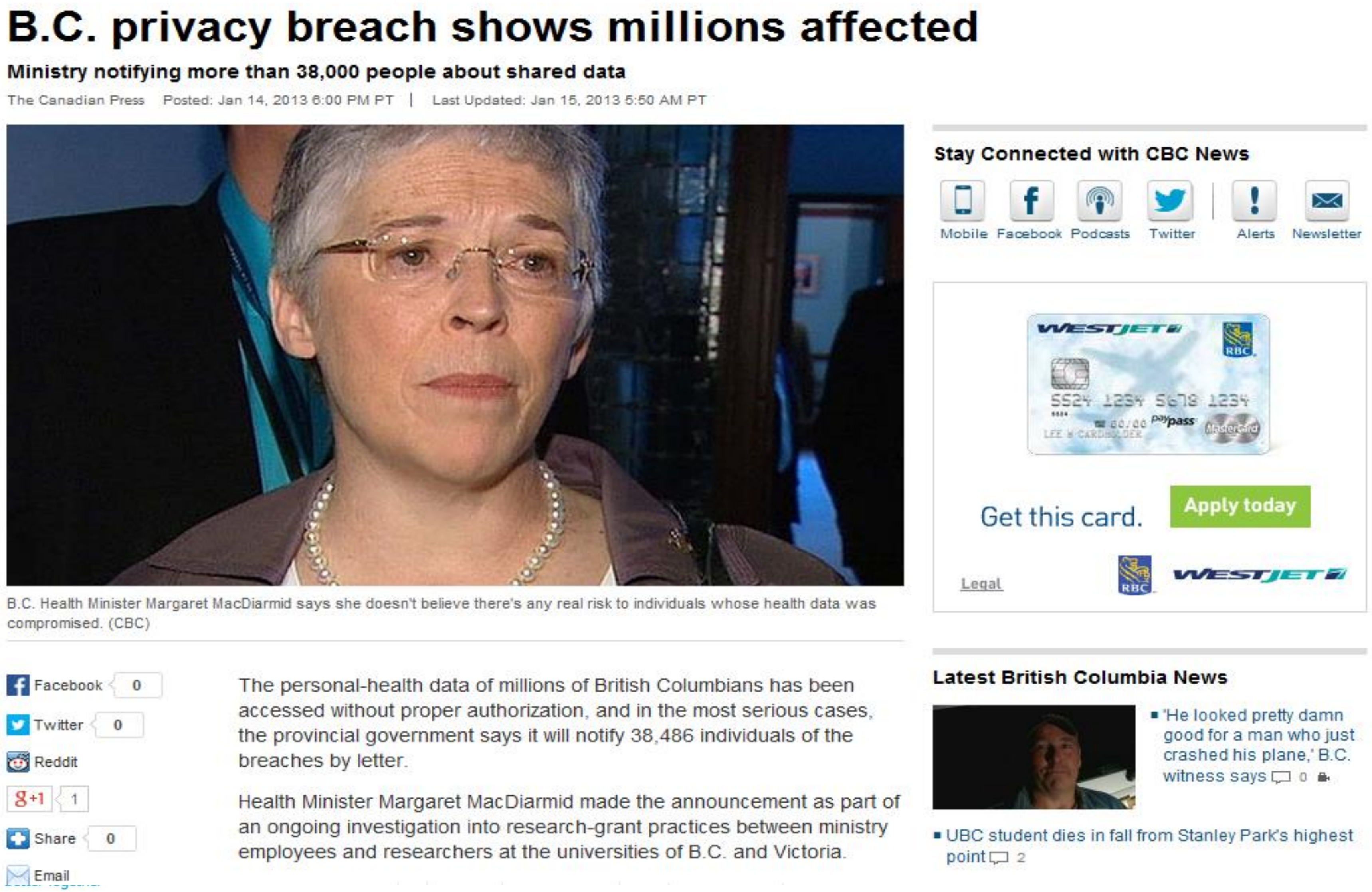
- "Just" viewing PHI (without a "need-to-know") is an unauthorized use and a serious breach.

Security Content

Part 3:

Research Security Content

We don’t want this to happen:



B.C. privacy breach shows millions affected

Ministry notifying more than 38,000 people about shared data

The Canadian Press Posted: Jan 14, 2013 6:00 PM PT | Last Updated: Jan 15, 2013 5:50 AM PT

B.C. Health Minister Margaret MacDiarmid says she doesn't believe there's any real risk to individuals whose health data was compromised. (CBC)

The personal-health data of millions of British Columbians has been accessed without proper authorization, and in the most serious cases, the provincial government says it will notify 38,486 individuals of the breaches by letter.

Health Minister Margaret MacDiarmid made the announcement as part of an ongoing investigation into research-grant practices between ministry employees and researchers at the universities of B.C. and Victoria.

Stay Connected with CBC News

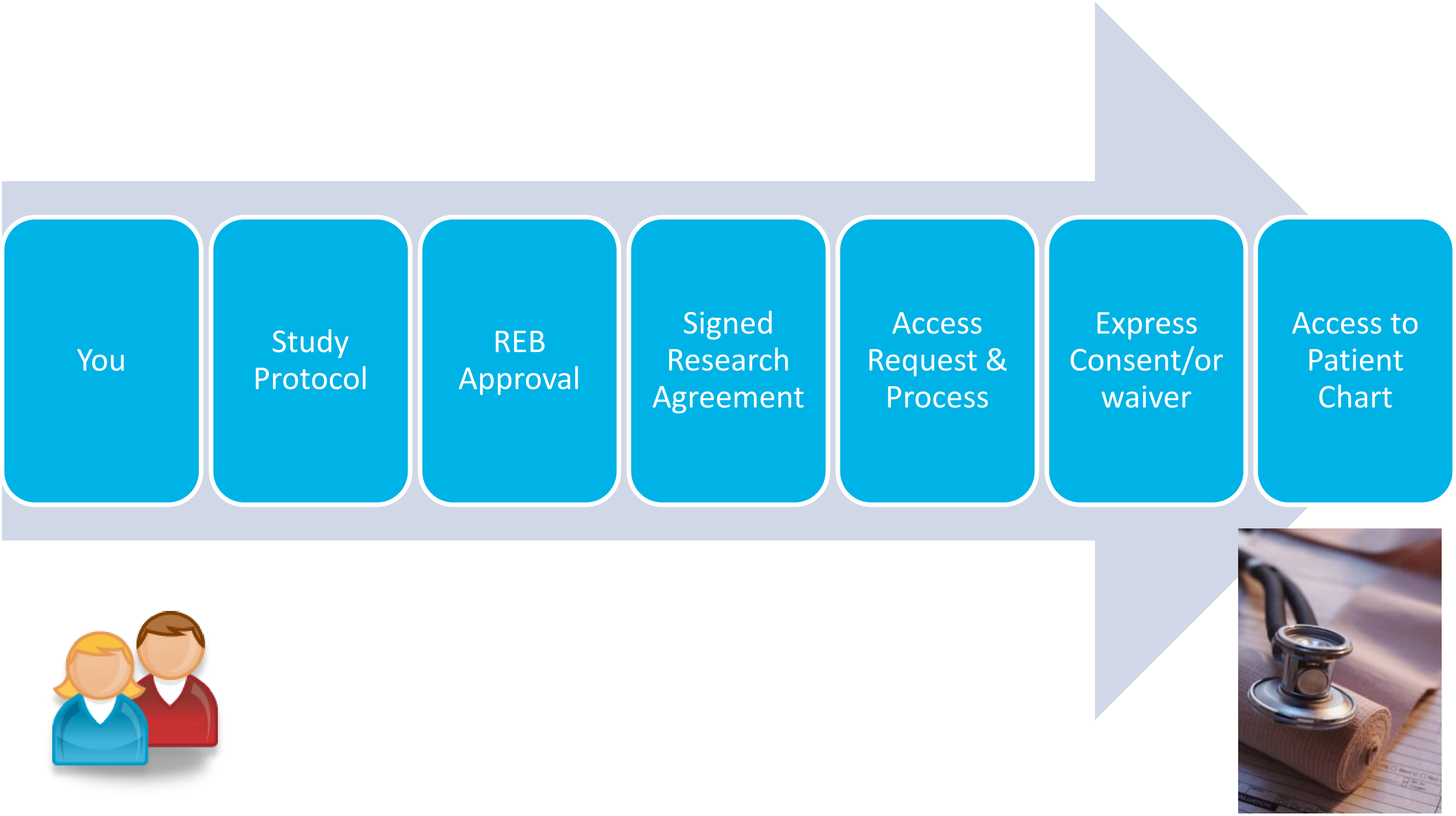
Latest British Columbia News

- 'He looked pretty damn good for a man who just crashed his plane,' B.C. witness says 0
- UBC student dies in fall from Stanley Park's highest point 2

Background: Access to PHI

- Access to Personal Health Information (PHI) for research purposes is strictly governed by the *Personal Health Information Protection Act* (PHIPA)
- THP **and** Researchers must be complaint, with REB approval and oversight
- When doing research, you can only access patient charts AFTER you have received approval from the THP Research Ethics Board (REB) in a way that had been approved
  - E.g., chart review or following express consent
  - And only after a Research Agreement has been signed

Research Access Overview



You

Study Protocol

REB Approval

Signed Research Agreement

Access Request & Process

Express Consent/or waiver

Access to Patient Chart

Access: Research Rules

- You must obtain and document a participant’s EXPRESS consent PRIOR to accessing their medical records; OR
- You must have obtained REB approved waiver of consent to access PHI for chart access

Before you get started…

- All access to patient records is routinely audited to ensure access is appropriate
- External researcher access to patient records is audited at an increased frequency
- Don’t snoop – your study may be suspended at THP and you’ll probably get fired

And don’t forget…

Inappropriate access can look like:

- Accessing a chart in advance of obtaining and documenting a participant’s express consent
- Using THP resources to access a participant’s information located at another health care facility
- Accessing and Using patient information in a way that is not in the approved Study Protocol

Therefore…

- Understand your THP-approved Study Protocol well
- Only access and use participant information in a way consistent with the approved Study Protocol
- Don’t access and use participant information until your study is REB-approved
- Access only after you obtain & document participant express consent
- For chart reviews, only access once waiver of consent is REB approved

Security Content

Part 3:

Core Security Content

Computer Security

DID YOU KNOW?
YOU PLAY A MAJOR ROLE IN COMPUTER SECURITY!

- Computer security protects the confidentiality, integrity, and availability of THP systems and data. Computer security enables privacy protection.

Good computer security protects:

- Personal Health Information (PHI)
- Corporate confidential information, including financial and HR data
- Research
- Intellectual property
- Privileged legal information

This is achieved by employing computer system safeguards, and by encouraging safe computing practices.

Computer Security – Become a knowledgeable user

A knowledgeable user is the best defense, and here's how you can help!

- ✓ Become familiar with THP computer security policies
- ✓ Managers should encourage staff to read, understand and follow the policies
- ✓ Employ good security practices in your daily work

THP Expectable Use Policy

What does this policy cover?

- Ensuring that we all use THP computer systems in an appropriate manner.

Why is this important?

- Inappropriate use exposes THP to security risks that could cause our systems to malfunction or result in privacy breaches. Examples include:
  - Computer viruses
  - Unauthorised access (hackers)
  - Corruption of patient information

THP Password Policy

What does this policy do?

- Ensure that we use computer passwords that are effective at preventing unauthorised access.

Why is this important?

- Passwords are an important aspect of computer security. They are the first line of protection for user accounts. A poorly chosen password may result in the compromise of the THP corporate network.

What can I do?

- Create 'strong' passwords by using a combination of upper & lower case, alpha/numeric, and special characters (Example: $uMm3r!, S@mplePa55word, P@ssphrase2Remember!)
- Protect your password by keeping it a secret and by not writing it down
- Do not re-use passwords
- Do not choose a new password that is similar to your old password
- Do not choose passwords that are easy to guess

THP E-mail & Internet Use Policy

What does this policy cover?

Complimenting the Acceptable Use Policy, the Email Policy and Internet Usage Policy provide detailed guidance on the appropriate use of these systems.

What are some examples of inappropriate use?

- Attempting to use the Internet to view inappropriate content, such as gambling, violent or sexual content web sites
- Unauthorised transmission of information that is proprietary or confidential to THP
- Transmission or transferring of PHI to an external recipient without appropriate protection (i.e. Strong encryption on all mobile devices including laptop, PDA, or USB key; password protecting Word, PDF and Zip files before sending)
- E-mail boxes being configured to automatically forward messages to external e-mail addresses

Good Security Practice Supports Privacy

User IDs, passwords, ID badges, access cards, and room keys are given to you for YOUR use only and are linked to your name and credentials.

- Don’t give your user IDs or passwords to others, and don’t use others’ IDs or passwords or encourage others to share their credentials.
- Remember that system access is logged and audited and you may be required to answer questions related to your access
- Immediately change your password if compromised
- Don’t use automated password-save features
- Always log out whenever leaving a computer, even for a short time. You can also lock the screen by holding down the Windows key and hitting the “L” key.
- Store ID badges and room keys separately (e.g. not on the same key ring). This prevents inappropriate access if lost or stolen.

Securing PHI

Secure Storage of PHI

- Store all clinical information in the chart
- Lock up paper records when unattended
- Save electronic files containing PHI to hospital network file; shared, authorized electronic systems, or to an <u>encrypted</u> mobile device, <u>**not**</u> on your desktop, hard drive or unencrypted device

Secure PHI Disposal

- Place all records for disposal containing PHI in corporate shredding bins (e.g. printouts from patient records, patient lists, and appointment schedules).
- <u>**Do not**</u> recycle or put paper with PHI in the regular garbage. Use locked shredding bins.
- Check with the Privacy Office (x7548) for disposal of CDs, video tapes, hospital cards, armbands & old electronics.
- Physically destroy USB keys or hard drives, or use software to securely 'wipe' them before permanent disposal.

Remember…

- Use only hospital-supported electronic devices for THP business purposes.
- Ensure all use of hospital and personal devices, systems and applications containing PHI complies with THP policies and all applicable laws.
- Report any device or record loss or theft to the Privacy Office <u>immediately</u>.

Sharing & Saving PHI

If **transmitting** or **transporting** PHI between authorized Hospital sites, organizations or people:

- Use secure methods of transmission (e.g. Fax, secure email or secure electronic file transfer)
  - Only send emails ***from*** a secure email address (e.g. trilliumhealthpartners.ca email) **and** *to* a secure email address.
  - Always double check the fax number or ‘To’, ‘Cc’, and ‘Bcc’ fields on emails before sending.

- Use **encrypted** electronic mobile devices (e.g. laptop) to transport data by hand or to send by courier.

- Keep biological samples, papers and electronic devices on your person as you move and be aware of their location at all times.

- Don’t leave PHI in your car or other public areas unattended.

Sharing & Saving PHI

- Assume other methods of communication, such as web-based services (e.g., Gmail, Dropbox, GoogleDocs) are NOT secure for PHI use. If using non-hospital systems/services, prior organizational approval (Privacy, Information Security and Chief Information Officer) and appropriate controls are required.

  - Don’t use other methods of communication even if the recipient is authorized to see the information (e.g., recipient is a patient or a patient’s external care provider) unless the patient has given express consent and acknowledged the risk of using the alternate communication method.

  - Patient express consent must always be obtained before emailing recipients such as a patient’s family or lawyer who are not authorized to get the information under implied consent.

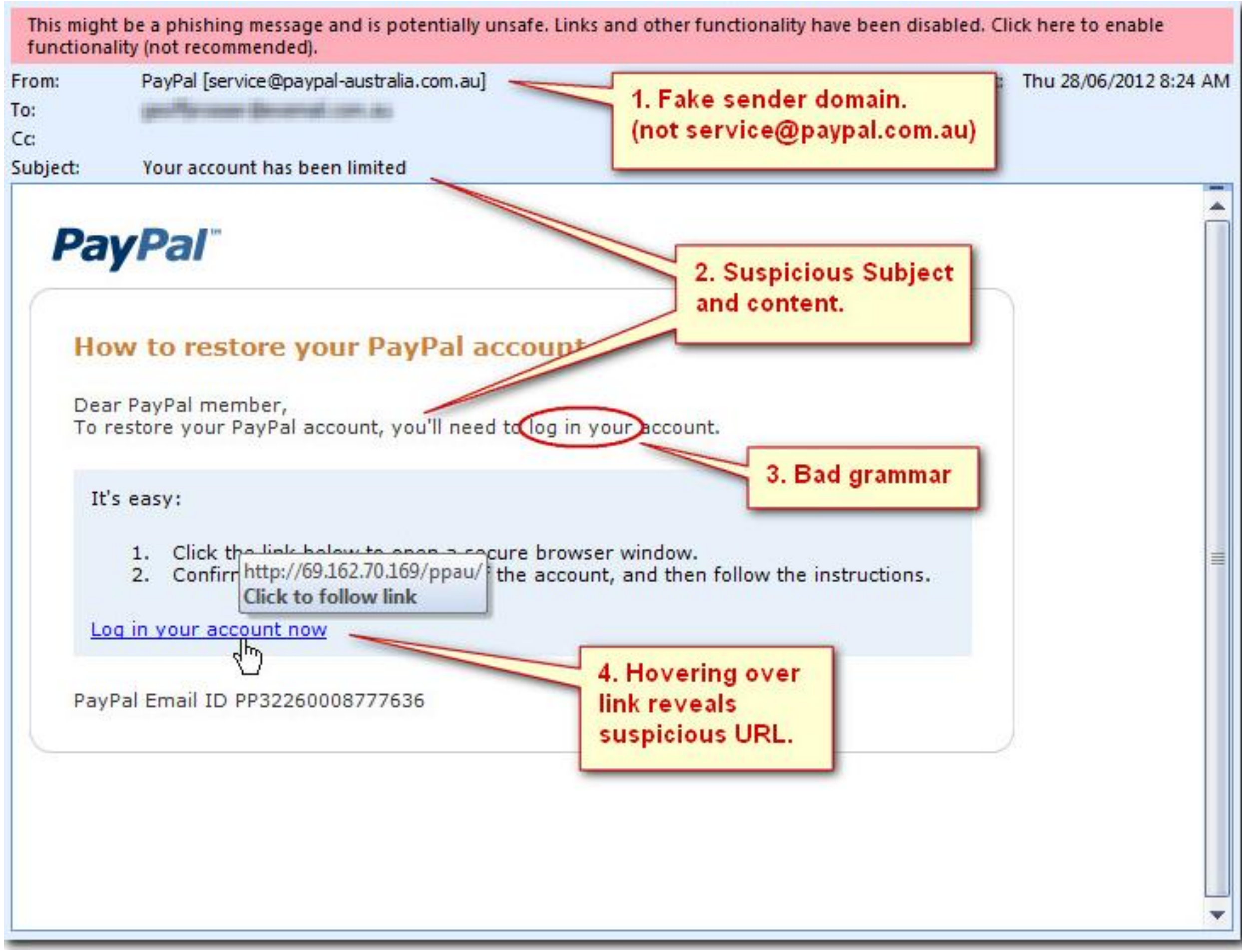
Safe Computing Practices

Phishing and Cybercrime

'Phishing' is a criminal activity carried out by fraudsters attempting to obtain sensitive information such as passwords , credit card details or PHI. Victims may stumble onto phishing web sites by mistyping a web address (URL) -- googl.ca instead of google.ca -- but usually they first receive email masquerading as official communication from a trusted source and are then directed to reply to the email or go to a phishing web site.

Phishing emails and web sites have become very sophisticated in appearance and are often difficult to distinguish from legitimate ones. Most create the impression that there is an immediate threat to one of your accounts (email, bank, etc.). Because of the supposed urgency victims often respond by supplying their sensitive information.

Sample Phishing Email



This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au]
To: [redacted]
Cc:
Subject: Your account has been limited

Thu 28/06/2012 8:24 AM

PayPal

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm the account, and then follow the instructions.

http://69.162.70.169/ppau/
Click to follow link

Log in your account now

PayPal Email ID PP32260008777636

1. Fake sender domain. (not service@paypal.com.au)

2. Suspicious Subject and content.

3. Bad grammar

4. Hovering over link reveals suspicious URL.

Phishing & Cybercrime

How to Avoid Phishing Scams

- Do not reply to any suspicious emails
- Delete requests for your password
- Be suspicious of any requests for financial information
- Don't click links or open files (ex. Zip, PDF, doc) in unexpected email, even from trusted senders. The following are safe alternatives:
  - Type the organization's main URL into your Web browser's address bar and navigate from there
  - Call the organization using a telephone number from a reliable source (i.e.: telephone directory or legitimate, printed, letterhead)
- Do not fill out forms embedded in email messages

Clean Desk Policy

- A clean desk policy reduces the threat of a security incident as confidential information will be locked away when unattended.

- Sensitive documents left in the open can be stolen.

- Take a few moments at the end of each day and put sensitive information in a locked drawer or filing cabinet.

Report Suspicious Events

- Help us protect our PHI by reporting unusual or strange computer activity
- Forward suspicious emails to the helpdesk for verification
- Don’t visit links in emails which send you to non-THP webpages
- Don’t open unexpected files (e.g.: Zip and PDF) in emails
- Report the use of computers by unknown persons to IT Security
- Report lost or stolen laptops, tablets, cellphones or other hospital issued devices to ISServiceDesk and Privacy Office immediately

Working with Vendors

When working with vendors and third parties, they need to demonstrate to you that they have equal or equivalent controls to THP when accessing PHI or systems containing PHI; for example, installing or updating billing systems.

- Ensure you have a contract in place that includes privacy & security protections, such as:
  - Security controls if they receive, transit or transfer PHI
  - Access controls if they support the system
  - Confidentiality agreements
  - Formal understanding of hospital information security policies

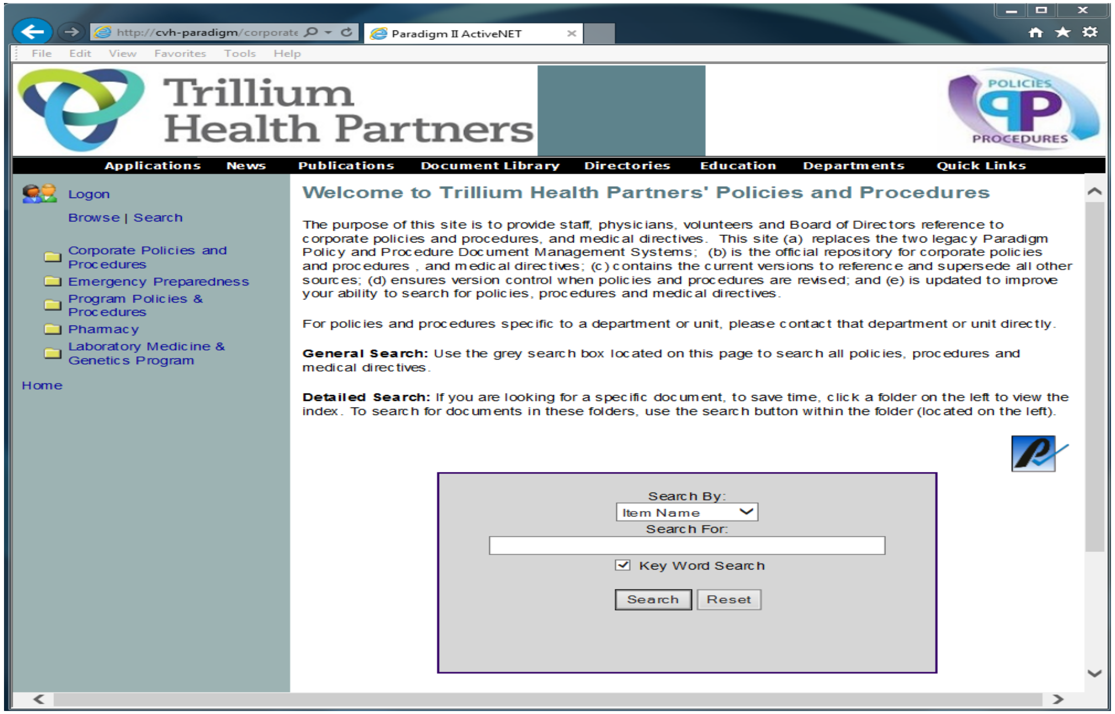
- If the vendor or third party is accessing a THP resource or environment, they may need to sign a separate access agreement

- If in doubt, ask the Privacy Office

Policies-Information-Resources

Looking for Information?

All THP Policies can be found on THPHub under Policies & Procedures > Corporate Policies and Procedures:


http://cvh-paradigm/corporate
Paradigm II ActiveNET
File Edit View Favorites Tools Help
Trillium Health Partners
POLICIES
PROCEDURES
Applications News Publications Document Library Directories Education Departments Quick Links
Logon
Browse | Search
Corporate Policies and Procedures
Emergency Preparedness
Program Policies & Procedures
Pharmacy
Laboratory Medicine & Genetics Program
Home

Welcome to Trillium Health Partners' Policies and Procedures

The purpose of this site is to provide staff, physicians, volunteers and Board of Directors reference to corporate policies and procedures, and medical directives. This site (a) replaces the two legacy Paradigm Policy and Procedure Document Management Systems; (b) is the official repository for corporate policies and procedures , and medical directives; (c) contains the current versions to reference and supersede all other sources; (d) ensures version control when policies and procedures are revised; and (e) is updated to improve your ability to search for policies, procedures and medical directives.

For policies and procedures specific to a department or unit, please contact that department or unit directly.

General Search: Use the grey search box located on this page to search all policies, procedures and medical directives.

Detailed Search: If you are looking for a specific document, to save time, click a folder on the left to view the index. To search for documents in these folders, use the search button within the folder (located on the left).

Search By: Item Name

Search For:

☑ Key Word Search

Privacy & Training for Shared Systems

Part 4:

Privacy and Security Training for users of Connecting GTA (cGTA), REACH and other shared systems

Access to Shared Systems

Why are you provided access to ConnectingGTA (cGTA) and other shared systems (such as REACH, PRO, Di-Repositories)?

- Because you are an ‘agent’ of THP, which is a participant in cGTA and other shared systems
- Because you need the PHI to provide or support the provision of patient care – cGTA and other shared systems are ONLY available for clinical care and must NOT be accessed for any other purposes including education, research, quality control, risk management or program planning.

THP’s Local Registration Authority (LRA) will provide you with access and revoke your access if you leave the organization.

Remember! Everything in the cGTA and other shared systems related to an identifiable individual is PHI (including provider name, payments, SDM name, OHIP information, visit information, etc.)

Protecting PHI

Remember! PHIPA set out the rules for protecting PHI and patient rights in all forms and these rules apply to PHI in cGTA and other shared systems

- THP must obtain patient consent prior to accessing PHI in cGTA and other shared systems
- Implied consent to access PHI in cGTA and other shared systems is obtained though THP's existing notices & processes
- Patients can withhold or withdraw consent for their PHI to be disclosed or collected in cGTA and other shared systems (usually called a 'consent directive' or 'lockbox')
- Patients can go to www.ConnectingGTA.ca or http://www.ehealthontario.on.ca/en/initiatives/resources for more information about cGTA, OLIS, and how to contact eHealth Ontario
- Patients can also go to www.trilliumhealthpartners.ca/Pages/Privacy.aspx for more information about other shared systems (such as REACH, PRO, DI-Repositories, etc.) and how to contact the THP Privacy Office for more information.

Withdrawn Consent

Can a patient withdraw consent?

- Yes, and this may block you from viewing the record
- If a patient has blocked information with a consent directive, the system will alert and instruct you
- Different systems allow for different types of consent directives
- If a patient does not want some or all of their PHI to be shared or is wondering why some or all of their PHI cannot be seen, contact the Privacy Office immediately (905)848-7580 ext.7548. Lab data stored in OLIS can only be blocked by calling Service Ontario

Can I view blocked data?

- Under PHIPA, you can override a lockbox in any one of the following situations:
  - Express consent obtained from patient (documented in chart)
  - Express consent obtained from Substitute Decision Maker (SDM) (documented in chart)
  - Significant risk of bodily harm
- If there are special rules within a shared system, the system will provide instructions (e.g. viewing blocked OLIS data in cGTA)

Patient Rights

Patients have the same rights around their PHI in cGTA, REACH, PRO, DI-Repositories and other shared systems, as they do over PHI in internal THP systems, including:

- Asking to see or get a copy of their information such as:
  - Their PHI
  - Audits of their PHI (including user names, actions, dates/times)
  - Consent directive history
- Asking to have PHI corrected if it is out-of-date or incorrect
- Asking a question or making a complaint to your organization or the Information and Privacy Commissioner of Ontario
- Asking to have their PHI not used or shared

You should contact the THP Privacy Office if a patient asks about any of the above.

Remember

To protect your access to shared systems, do the same as you would when accessing an internal THP system:

- Only use your credentials to log in and do not allow others to use your credentials
- Create ‘strong passwords’ (i.e. 8 or more characters, with special characters, that are not easy for others to guess), different from passwords for personal accounts (e.g. online banking, email)
- Change password immediately if it may have been compromised
- Do not include your credentials in an automated sign-on process (e.g. stored in a macro or function key)
- Log out of the system when complete
- Lock your workstation if you are logged into a system but need to leave your workstation unattended
- Cooperate with any audits of your activity
  - All activity in these systems is logged and privacy and security policies require regular audits to be run. This means that the Privacy Office may need your help to validate that your accesses to a system are only based on providing or assisting in the provision of healthcare
- Agree to all End User Agreements that you are presented with

Remember

You are responsible for protecting the PHI accessed through shared systems

To protect the PHI in shared systems, use the same security practices as you would when accessing an internal THP system:

- Only use devices approved by THP to access systems.
- Only use THP-approved remote access methods (e.g. VPN) and follow the proper process to disconnect from the remote connection when finished .
- Do not access systems in public areas where unauthorized individuals can view the information (e.g., Internet cafés, public transit, and other non-private settings).
- Do not leave your mobile computing device unattended in a public place, and lock it in a trunk or out of sight **before** getting to your destination if in a car.
- Do not try to disable, override or willfully bypass any security control, attempt to exploit any suspected security weakness, or knowingly perform an act that will interfere with the normal operations of a system

Remember

You are responsible for reviewing and following the OLIS Health Care Provider Guide:

http://www.ehealthontario.on.ca/images/uploads/initiatives/resources/olis_provider_guide.pdf

To protect the PHI extracted from shared systems, use the same practices as you would for PHI from an internal THP system:

- Do not take pictures or screenshots of the PHI displayed in a system.
- Only print PHI where there is a print button in the system and only print what is needed for a specific task.
- If PHI is downloaded, ensure that (1) only a minimum amount of PHI is copied, (2) the device is encrypted if it is a mobile device, and (3) PHI is either saved to a location where other records are saved or is removed/deleted when no longer needed
- Use your THP or ONEMail email account to send PHI to the cGTA help desk, eHealth Ontario, REACH or to another support email

Shared Systems – Privacy Breaches

What if there is a privacy breach or security incident in ConnectingGTA , REACH, PRO, DI-Repositories or another shared system?

Report the incident immediately to the THP Privacy Office

- Your site will report privacy breaches to eHealth Ontario and security incidents to the cGTA, REACH or other program team
- You may be required by your site to participate in an investigation
- If you are responsible for the incident, you will be subject to your site's policies and procedures for any remediation or discipline (*Note: your College may also take disciplinary steps and eHealth Ontario may remove your cGTA access.)*

What is a Privacy Breach?

- Any contravention of a privacy provision in PHIPA, agreements, or the privacy policies,
- When PHI is lost, stolen, or accessed by an unauthorized person, OR
- When PHI is copied, modified or disposed of in an unauthorized manner
- *Examples: Viewing PHI for a reason other than care; losing a printout of PHI*

What is a Security Incident?

- Any violation or imminent threat of violation of an information security policy, procedure or practice
- *Examples: sharing your password; suspecting that someone else has been using your login ID*

Disclaimer RE cGTA Data

PHIPA requires participants to take reasonable steps to ensure that PHI is as accurate, complete and up-to-date as necessary for the purposes for which it is being used.

The Connecting GTA Solution is new and as a result there is not yet a significant history of meeting that standard.

This is a factor that Clinicians should consider in deciding whether to validate PHI collected from cGTA against PHI in source systems before relying on it to make clinical decisions.

Annual Confidentiality Page

1. During the course of employment or other association with Trillium Health Partners ("THP"), I acknowledge that I will become aware of information in recorded or unrecorded form, expressly marked confidential or not, that is not generally available to the public and is generated, collected or used in the course of operating THP business activity, research and development activity, and the treatment of patients ("Confidential Information").

2. Confidential Information includes but is not limited to THP administrative and financial information, patient's personal health information and employee personal information. I shall not read records or discuss, divulge, or disclose such Confidential Information, unless there is a legitimate purpose related to my employment role, privileged physician role, volunteer role, agency role or other association with THP, as applicable. This obligation does not apply to information in the public domain. I shall not remove Confidential Information from THP premises except when necessary for the provision of health care, other permitted purposes noted in the *Personal Health Information Protection Act, 2004* ("PHIPA"), or when required for the purposes of my employment. When in transit, I shall securely store and ensure the Confidential Information is in my custody and control at all times. If Confidential Information must be removed from THP, I shall ensure it is "de-identified" where possible. De-identification means deleting or removing personal identifiers to prevent personal health information or personal information from being connected with an identifiable individual.

Annual Confidentiality Page

3.   I understand the purposes for which agents of THP are permitted to collect, use and disclose personal health information.

4. I understand and agree that agents of THP are prohibited from: (i) collecting, using or disclosing personal health information if other information will serve the purpose; and (ii) collecting, using or disclosing more personal health information than is reasonably necessary to meet the purpose.

5. I shall ensure that Confidential Information is not inappropriately accessed, used, or disclosed either directly by me, or by virtue of my signature or security access to premises or systems.

6. Violations of this agreement include, but are not limited to:

- accessing information that I do not require for performing my duties at THP;
- misusing, disclosing without proper authorization, or altering patient or personnel information; and
- disclosing to another person my user name and/or password for accessing electronic records or other electronic systems.

Annual Confidentiality Page

7. I shall only access, process, and transmit Confidential Information using hardware, software, and other THP authorized equipment, as required by the duties of my position. I shall store all electronic Confidential Information on a THP secure network or THP encrypted device.

8. I shall immediately report all lost or stolen Confidential Information, and that which is disclosed, accessed or used in an unauthorized manner, to my immediate supervisor and to the THP Privacy Office.

9. I understand that THP will conduct regular audits of access to THP electronic systems to ensure compliance with this agreement and its privacy and confidentiality policies.

10. I understand and agree to abide by the conditions outlined in this confidentiality pledge, and they will remain in force even if I cease to have an employment or other association with THP.

11. I agree to securely return all property of THP including keys and records of personal health information, if any, at the conclusion of my employment, contractual, volunteer, privileged or other relationship with THP.

Annual Confidentiality Page

12. I acknowledge and agree that I have read and understood and I will at all times during the period of employment comply with THP's Code of Conduct and privacy and confidentiality policies as they relate to Confidential Information and that I understand my obligations under and will comply with applicable privacy legislation, including the Personal Health Information Protection Act, 2004.(Ontario).

13. I also understand that should any of these conditions be breached, I may be subject to corrective action up to and including suspension or termination of my employment, privileged physician status, volunteer status, agent status or other association with THP, as applicable and a report to my regulatory college, if applicable.

Want More Information

Call the THP Privacy Office (905)848-7580 ext. 7548 or email privacy@trilliumhealthpartners.ca with any questions.

Visit the THP webpage on cGTA for cGTA specific information.

Visit http://www.ehealthontario.on.ca/en/initiatives/resources for more information about the larger cGTA project or to obtain a copy of the relevant privacy and security policies and agreements.

Remember to review and follow the OLIS Health Care Provider Guide at http://www.ehealthontario.on.ca/images/uploads/initiatives/resources/olis_provider_guide.pdf for rules about OLIS.