NORTH YORK GENERAL

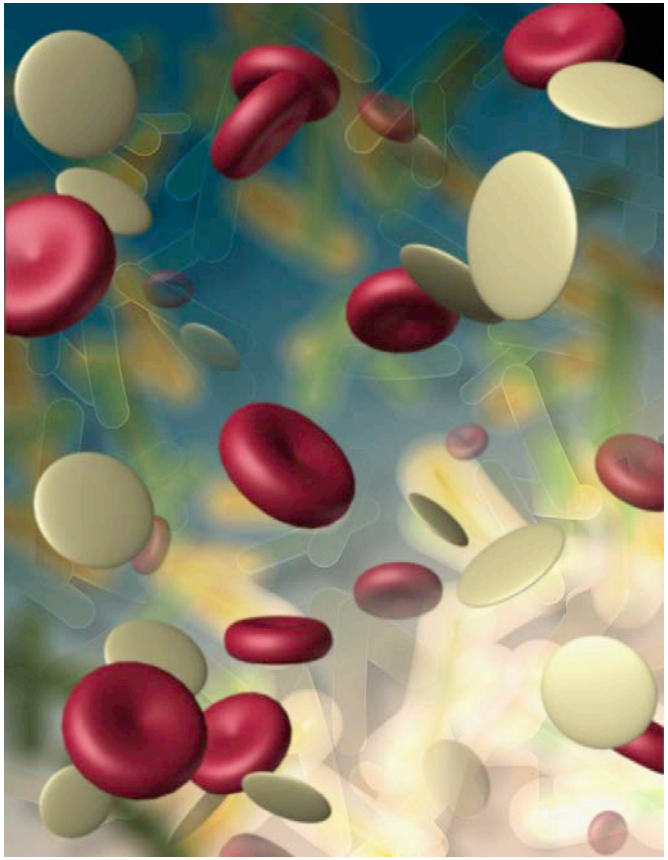
Making a World of Difference

PRIVACY & SECURITY FUNDAMENTALS FOR RESEARCHERS

NORTH YORK GENERAL

Making a World of Difference

Presentation Overview



- Privacy of personal health information (PHI)
- Governing authorities
- Protocol adherence
- Consent obligations
- De-Identification tips
- E-mail security
- Safeguarding devices
- Encryption tips
- Disseminating findings
- Additional resources

NORTH YORK GENERAL

Making a World of Difference

Privacy

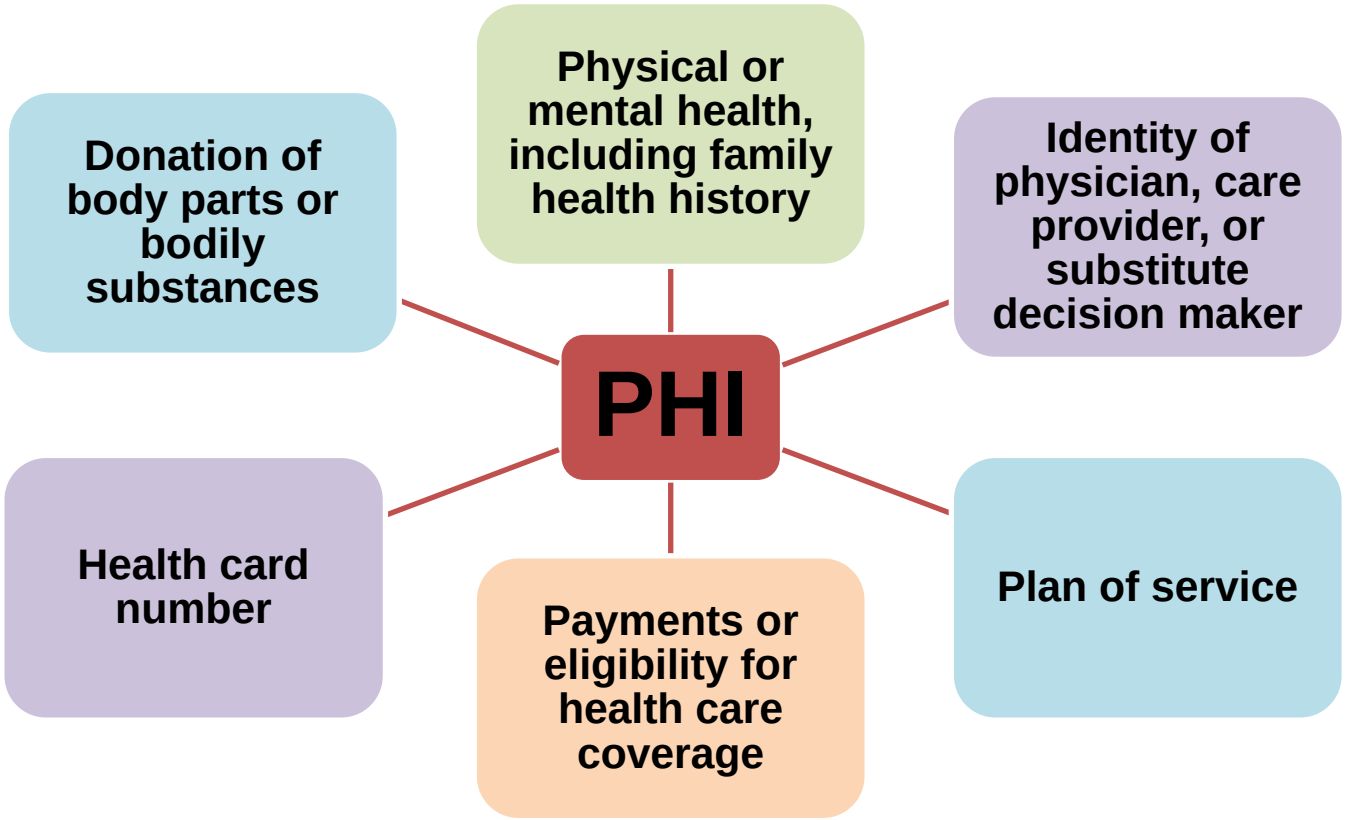
Fundamental human right & legal obligation; internationally recognized norm & ethical standard

Ontario's *Personal Health Information Protection Act, 2004* **(PHIPA) governs** the collection, use and disclosure of PHI for research purposes

NORTH YORK GENERAL
Making a World of Difference

Personal Health Information (PHI)

PHI: identifying information in oral or recorded form that relates to any of the following about an individual



NORTH YORK GENERAL

Making a World of Difference

Alignment with Research Authorities, Public Expectations

In addition to PHIPA privacy rules, the following also require privacy protection as a **condition for conducting research**:

- Research Ethics Boards (REB)
- TAHSN Research Ethics Committee
- Tri-Council Policy Statement (TCPS)
- NYGH policies
- Professional College guidelines
- OHRP
- FDA

Adherence to these standards protects patients and you

NORTH YORK GENERAL

Making a World of Difference

Research Planning

Provide for protecting privacy and security at **all phases** of the research process including:

- Identification/selection of study subjects
- Communication with research team
- Recruitment
- Consent procedures
- Data collection procedures
- Data storage
- Analysis
- Dissemination/ publication
- Retention
- Disposal

NORTH YORK GENERAL

Making a World of Difference

Protocol Obligations

No deviation from protocol

Contact patients to request consent to participate **after** REB approves study

Collect minimum (PHI) necessary and use only for approved purposes

Implement safeguards outlined

Disclose PHI only to authorized recipients identified in protocol

Where possible, de-identify PHI by removing/changing information so individuals cannot be identified

NORTH YORK GENERAL

Making a World of Difference

Connecting Ontario – Shared Systems

No access permitted for research purposes

Shared health systems may <u>only</u> be used for the purpose of providing care or assisting in care provision

Privacy breach : accessing cGTA or other shared systems (OLIS, HDIRS, IAR etc.) for research purposes

Required Notice: to Information & Privacy Commissioner, patients, Chair of Research Ethics Board; Colleges may be notified, potential for fines, civil action for privacy breach

NORTH YORK GENERAL

Making a World of Difference

Consent Obligations

Obtain express patient consent to collect PHI **unless** REB has waived consent obligation

REB may waive consent where:

1. Research purposes can be achieved without identifiable information

2. Impractical to obtain consent

3. Public interest in conducting the research exceeds the public interest in protecting the privacy of the individuals; and

4. Information is protected by adequate safeguards

NORTH YORK GENERAL

Making a World of Difference

De-identification

PHI must be de-identified:

- Before removal from a hospital site or network
- Before disclosure to a contractor or external member of research team (e.g. statistician) or to a sponsor or offsite monitor
- Before publishing or presenting unless patients have provided written consent

Best Practice: de-identify before importing to statistical or other software/tools

NORTH YORK GENERAL

Making a World of Difference

De-identification Tips

Removing/changing information so that individuals cannot be identified

Generate a unique study ID number for each participant (do not use initials, OHIP, MRN or DOB)

Remove unique identifiers from data

- Name/Telephone/Fax number/DOB
- Address, forward sortation postal code
- Emergency Contact/Next-of-kin
- Hospital number/OHIP number
- IP/email addresses
- Biometric identifiers
- Photographs and identifying images

Remove quasi identifiers from the data

- Physician name (if prominent)
- Clinic name (if linked to condition)
- Geographic location
- Name of rare disease
- Unique personal characteristic
- Qualitative comments

Create a study identification code list that contains participants' study IDs and any identifiable information, including unique and quasi identifiers that were removed (list must be securely stored)

Use the study ID on all study documents (other than source files)

Correct for small sample/cell sizes when publishing or presenting results to decrease possibility of outliers or unique cases being re-identified based on inference even when names, other unique identifiers are not included

Use age or year of birth rather than collect DOB unless strictly necessary

Use De-identification Software
(not an exhaustive list of methods)

NORTH YORK GENERAL

Making a World of Difference

Safeguarding PHI on Devices

Avoid using mobile devices/removable storage media to store/transport PHI

E.g. - Laptops, tablets, smartphones, USB flash drives, optical discs (CDs, DVDs), memory cards (SD, CF, etc.),external hard drives

If necessary to store/ transport PHI using such devices, physical, technical and administrative safeguards must be employed; **minimum requirement - encrypted files, whole disk encryption is best practice**

NORTH YORK GENERAL

Making a World of Difference

Safeguarding PHI on Devices

Consider Secure Alternatives: Is there a secure alternative that would allow you to complete the work without storing PHI on your device (e.g. remote access)?

Authorization to Store/Transport PHI: Are you authorized to store or transport PHI on devices?

Minimize or De-identify PHI: Have you stored the least amount of PHI possible and used de-identified data when it will serve the purpose?

Whole Disk Encryption & Passwords: Is the PHI protected from unauthorized access both by whole disk encryption **and** strong passwords?

Avoid Unsecured Networks:
Do you use secure networks/protocols when sending or receiving PHI on your device?

NORTH YORK GENERAL

Making a World of Difference

Safeguarding PHI on Devices

Know the PHI: If your device is lost or stolen, could you identify all the PHI stored on it?

Use Protective Software & Configure Your Device Settings: Have you installed and are you using up-to-date firewalls, anti-virus and anti-theft software?

Be Aware of Physical Security: Do you transport/use devices in a secure manner to prevent loss, theft, "shoulder-surfing" or eavesdropping? Do you take the most direct route and keep things locked up?

Report Immediately Losses or Theft: If it occurs, do you know who to contact to report the loss? (NYGH's Chief Privacy Officer (CPO): Rita Reynolds)

Remove PHI from your Device as Soon as Possible: Do you securely remove all PHI stored on your device as soon as possible?

NORTH YORK GENERAL

Making a World of Difference

Emailing PHI to Research Team

Only use secure system to transmit PHI i.e. a system that automatically encrypts data during transmission

Secure transmission: e.g. between ONE Mail users; between NYGH email users

Never send PHI to personal accounts: gmail, hotmail etc.

System not secure: send only de-identified data that has been encrypted & protected by strong password

- Note: encryption protects against re-identification if data is lost/stolen

NORTH YORK GENERAL

Making a World of Difference

Encrypting Files

PHI on mobile devices/removable storage media is **not allowed** unless encrypted

Make sure you are encrypting a copy of the original and not the original or else you will always have to use a password to open originals stored on secure networks/servers

Create a strong password. Write it down. Send the file to the recipient and explain that the password will be sent in a separate email. They can just copy and paste the password to open the document. If retaining password, store securely

NORTH YORK GENERAL

Making a World of Difference

Microsoft Word

How to encrypt a Word 2010 document:

- Click the **File** tab
- Click **Info**
- Click **Protect Document**, and then click **Encrypt with Password**
- In the **Encrypt Document** box, type a password, and then click **OK**
- In the **Confirm Password** box, type the password again, and then click **OK**

NORTH YORK GENERAL

Making a World of Difference

Microsoft Excel

How to encrypt an Excel 2010 file:

- Click the **File** tab
- Click **Info**
- Click **Protect Workbook**, and then click **Encrypt with Password**
- In the **Encrypt Workbook** box, type a password, and then click **OK**
- In the **Confirm Password** box, type the password again, and then click **OK**

NORTH YORK GENERAL

Making a World of Difference

Microsoft Access

How to encrypt an Access 2010 database:

- Open the database in **Exclusive** mode
- Click the **File** tab
- Click **Info**
- Click **Protect Workbook**, and then click **Encrypt with Password**
- In the **Encrypt Workbook** box, type a password, and then click **OK**
- In the **Confirm Password** box, type the password again, and then click **OK**

NORTH YORK GENERAL

Making a World of Difference

Adobe PDF

Encrypting an Adobe PDF file (requires Adobe Acrobat Pro):

- Click the **Tools** pane
- Open the **Protection** panel
- Click **Encrypt** and select **Encrypt With Password**
- Confirm that you want to change the security of the document
- In the **Password Security Settings** dialog box you can add two types of passwords
  - The **Document Open** password restricts who may open the document
  - The **Permissions** password restricts printing, editing and copying based on your selections
- Click **OK** and confirm the password(s) chosen
- Save the document to apply the new security settings
- Type a name for your file and click **Save**

NORTH YORK GENERAL

Making a World of Difference

Encryption Checklist

- ❑ I have minimized the amount of PHI on mobile devices and removable storage media and it is stored in encrypted form
- ❑ I use a strong password to protect the encrypted data AND it is different than the password that I use to login to my computer
- ❑ Best practice: I have purchased software to implement **whole disk encryption** on my device , or I buy devices with whole disk encryption already installed
- ❑ I have enabled my operating system encryption
- ❑ I never write my password down unless it is stored under lock and key or in such a manner that it is very secure e.g. encrypted file list
- ❑ I do not share my password with anyone
- ❑ I delete PHI from all mobile devices and removable storage media once I have finished working with it
- ❑ **Please note:** PHI should be deleted/erased from mobile devices in such a manner that reconstruction of the data is not reasonably forseeable in the circumstances

NORTH YORK GENERAL

Making a World of Difference

Disseminating Findings

De-identified, aggregated data must be used for presentations/publications unless participants' express consent sought and documented

Never reveal identities of non-consenting participants; participants may be recognizable even when direct identifiers are removed

NORTH YORK GENERAL

Making a World of Difference

Providing PHI to Participants

Not required but may support clinical care/research relationship if access consistent with REB approved protocol

Ask for consent before giving any information to participants' family or friends and before leaving a detailed voicemail

Refer requests for clinical non-research information to NYGH's Release of Information department

NORTH YORK GENERAL

Making a World of Difference

Retaining & Disposing of PHI

Select secure location for retention;
Use a hospital or other secure network for electronic files

At end of retention period, confirm destruction plans with sponsor, securely destroy identifiable data to avoid recovery

- Don’t recycle or trash materials
- Cross-cut shred paper, disks, CDs, DVDs
- Destroy USB keys/hard drives or use software to securely wipe
- Obtain certificates of destruction from any vendors that assist you

NORTH YORK GENERAL

Making a World of Difference

Information & Privacy Commissioner/Ontario (IPC)

This tribunal provides oversight of compliance with the Personal Health Information Protection Act. In this role the Commissioner:

- adjudicates access appeals, investigates privacy complaints and may issue public reports
- may enter and inspect premises, records, information management practices and require evidence under oath, affirmation
- has Order making power; may levy fines of up to $250,000.00

IPC Contact: 416-326-3333 www.ipc.on.ca

NORTH YORK GENERAL

Making a World of Difference

ATTESTATION OF COMPLETION

I hereby attest that I have completed Privacy & Security Fundamentals training for Researchers. I understand that this attestation is valid for one year. After expiry, the training must be redone and a current attestation submitted for any new studies.

Name:

Institution:

_____ _____

Date **Signature**

*Please print this form and sign. A hard copy of the signed attestation **must be** submitted with your application for REB approval. Keep a copy for your record as it may be used for new studies submitted prior to the one year expiry date.*

NORTH YORK GENERAL
Making a World of Difference

Additional Information

Please take some time to familiarize yourself with the following resources:

NYGH Policies

Mobile Devices, Removable Storage Media, and Personal Health Information Security

Privacy & Data Protection

Disclosure of Personal Health Information

NORTH YORK GENERAL

Making a World of Difference

Thank you

For more information please contact Rita Reynolds, Chief Privacy Officer at (416) 756-6448