Clinical Research Privacy Training
Introduction & Objectives

Introduction
This training is mandatory for all staff involved in clinical research.

Objectives
The learner should gain a better understanding of privacy as it relates to clinical research, specifically:

• Governance of research privacy
• Circle of care definition
• Need for expressed consent to contact for research purposes
• Protection of data
• Privacy breaches
What is privacy?

The right for an individual to determine who knows what about him/her and what they do with the knowledge.
What legislation is in place to govern privacy in clinical research?

- **Personal Health Information Protection Act (PHIPA)**
  - The law, developed in 2004, governs the way in which personal health information (PHI) can be accessed, collected, used and disclosed
  - It ensures the right to access one's own PHI
  - It is enforced by the Information and Privacy Commissioner’s (IPC) Office of Ontario
  - It is the responsibility of the Health Information Custodian (HIC) to protect the information
  - **Different rules apply for research purposes**

- **Other governance in research privacy:**
  - ICH E6(R2) GCP Guidelines: International Council for Harmonisation Guideline for Good Clinical Practice
Privacy Policies

The University of Ottawa Heart Institute (UOHI) and The Ottawa Hospital (TOH) have a number of policies related to privacy, including but perhaps not limited to:

• UOHI Privacy 1-200/TOH Privacy 00175
• Passwords, UOHI Policy 5-30
• Email Access & Usage, UOHI Policy 5-100
• Data Governance, UOHI Policy 5-140
• Corporate File Retention and Destruction, UOHI Policy 1-140
• Freedom of Information Requests, UOHI Policy 1-160
• Faxing Confidential Information, TOH Policy 00182
• Locking Patient Health Information Records, TOH Policy 00205
• Patient Anonymity Request-Privacy Level Code, TOH Policy 00633
• Social Media, TOH Policy 00672

You should familiarize yourself with these policies which can be found posted on the Heart Hub and on the TOH internal website.
OHIRC Privacy Policies & Other Governance

The Ottawa Heart Institute Research Corporation (OHIRC), the research arm of the UOHI, also has privacy policies, SOPs and other governance in place:

**Policies**
6-10 Ethical Conduct of Research  
6-40 Research Involving Humans  
6-90 Responsibilities of Principal Investigators  
6-160 Data Security & Confidentiality for Clinical Research Databases

**Clinical Research SOPs**
C-1-002 Regulatory Requirements & Essential Documents  
C-1-003 Privacy and Confidentiality  
C-1-004 Research Team Roles & Responsibilities  
C-1-005 Staff Training  
C-1-009 Data Sharing Agreements  
C-3-003 Master Subject List Requirements  
C-3-004 Source Documentation  
C-3-006 Management of Clinical Research Databases
Research Ethics Board

Provides oversight by reviewing and approving the Privacy Plan submitted with the study application.

Security and Systems Access (SSA)

Ensures each new worker at UOHI reviews the expectations for privacy by obtaining a signature on the Acknowledgement and Confidentiality Agreement.
PHIPA & Research

PHIPA specifically addresses disclosure for research in Section 44:

(1) A health information custodian (HIC) may disclose personal health information (PHI) about an individual to a researcher if the researcher,

(a) submits to the custodian (TOH/UOHI have delegated this responsibility to the Research Ethics Board (REB)):
   (i) an application in writing,
   (ii) a research plan that meets the requirements of subsection* (2), and
   (iii) a copy of the decision of a REB that approves the research plan; and

(b) enters into the agreement required by subsection (5). [confidentiality agreement]

* (most commonly referred to as the “Privacy Plan”)
In terms of the REB’s role, Section 44 states:

(3) When deciding whether to approve a research plan that a researcher submits to it, a REB shall consider the matters that it considers relevant, including,

(a) whether the objectives of the research can reasonably be accomplished without using the PHI that is to be disclosed;
(b) whether, at the time the research is conducted, adequate safeguards will be in place to protect the privacy of the individuals who PHI is being disclosed and to preserve the confidentiality of the information;
(c) the public interest in conducting the research and the public interest in protecting the privacy of the individuals whose personal health information is being disclosed; and
(d) whether obtaining the consent of the individuals whose PHI is being disclosed would be impractical.
Under PHIPA the researcher must be compliant as follows:

(6) A researcher who receives PHI about an individual from a HIC under subsection (1) shall,

(a) comply with the conditions, if any, specified by the research ethics board in respect of the research plan;

(b) use the information only for the purposes set out in the research plan as approved by the research ethics board;

(c) not publish the information in a form that could reasonably enable a person to ascertain the identity of the individual;

(d) despite subsection 49 (1), not disclose the information except as required by law and subject to the exceptions and additional requirements, if any, that are prescribed;

(e) not make contact or attempt to make contact with the individual, directly or indirectly, unless the custodian first obtains the individual’s consent to being contacted; (Referred to as expressed consent, which is explained in the coming slides)

(f) notify the custodian immediately in writing if the researcher becomes aware of any breach of this subsection or the agreement described in subsection (5); and

(g) comply with the agreement described in subsection (5).
Circle of Care

This term is not defined in the PHIPA legislation, yet is used frequently in reference to research privacy and confidentiality.

Only those who would normally have access to the patient’s PII/PHI, and be in contact with the patient, for the purpose of providing health care are considered part of the “circle of care”. This includes treating physicians, nurses, technicians, and registration clerks or administrative assistants managing patient testing or visits.

Research staff are NOT considered part of the circle of care and must not approach or contact patients without their prior expressed consent provided to the HIC.
Permission to Contact Process

To facilitate research, TOH and UOHI collaboratively developed a process to obtain a patient’s permission to be contacted for research purposes.

Registration Clerks at outpatient units obtain permission by following an approved script:

**What Do I Say to the Patient?**

“As you probably know we do a lot of research here. If we have a study that may be appropriate for you, is it ok if our research staff contact you?”

If they agree right away, stop here and enter decision in SMS; if they hesitate or ask for more information, proceed with the following:

“Saying ‘yes’ means you may be contacted, but it doesn’t mean that you are agreeing to participate in research. It just allows our research staff to contact you to explain research studies that may apply to you.”

Either way, then follow with:

“Here is a FAQ sheet that provides more detailed information for you.” (Patient is provided a handout which includes contact information for the UOHI Privacy Officer)

There are four possible entries into vOACIS by the clerk:

“Yes”, “No”, “Ask Another Time” (had the discussion but the patient was unable to decide or too overwhelmed to consider), or “Unable to answer” (if their current state prohibited the discussion)
Once the patient provides his/her permission to be contacted (PTC) to the registration clerk, it is visible in real time under “Alerts” in the patient’s vOACIS medical record, as demonstrated in the picture to the right.

The permission does not expire, however for respect of the patient, he/she will be asked again at their first visit after three years from the last permission.
Managing Research Data

• As previously explained, the HIC (TOH/UOHI) delegates the protection of patient privacy and confidentiality for research related activities to the Research Ethics Board (REB) (Ottawa Health Science Network Research Ethics Board (OHSN-REB) or a Board of Record through the Clinical Trials Ontario (CTO) Streamline Ethics System)

• Investigators must detail their Privacy Plan in the REB application, and obtain approval

• Research data leaving the HI should be de-identified / coded (strip the identifiers ASAP)

• Sharing data with external Investigators typically requires a Data Sharing Agreement or a Contract (even sharing between TOH and UOHI requires an agreement)

• Data collected at UOHI is the property of the Institute and must remain here, e.g.: may NOT be removed with trainee/fellow/researcher departure
Managing Research Data Con’t

The Informed Consent Form (ICF) must disclose to study participants all plans for the PHI

- What data will be accessed, used and disclosed
- Who will have access to the PHI
- How and where it will be stored – hard copies and electronic records
- What safeguards are in place for its protection
- What will be released to the Sponsor of the study and how it will be transferred
- How long the information will be saved and how it will be disposed/deleted
Reminders for Protecting PHI

Physical Protections
- Locked offices with restricted access, locked filing cabinet
- Minimal hard copy records – do not print copies from electronic medical record unless absolutely needed; the electronic version is the official record
- PHI must be stored separately from de-identified, coded study/research records (e.g., signed consent forms, demographic pages, etc. must be separated from the case report forms)

Administrative Protections
- Limit access to only those who need it
- Governing Policies and Procedures as discussed above, compliance is assessed with internal auditing practices

Technological Protections
- Store PHI only on hospital secure network drives – NEVER the C drive or a personal mobile device (unless permission has been explicitly granted to use a UOHI encrypted device)
- Encryption and strong passwords
Email & Faxing

Email

• PHI can only be sent internally and to a secure (UOHI or TOH) email recipient that has a need to know
• Do NOT include PHI in subject line
• If identity must be shared, wherever possible use the MRN and initials rather than name
• If possible, have PHI in a separate password protected attachment – and provide password in a separate email or by phone
• ALWAYS verify the “To” field before sending

Faxing

• Use a formal fax cover letter if the fax is going to an external fax machine
• ALWAYS verify the fax number before sending
• If you are expecting a fax containing PHI, wait by the fax machine to receive it
• ** Considered safer than email by the Office of the IPC of Ontario
What is a privacy breach?

The unauthorized access, collection, use, or disclosure of any personal information or personal health information.

• A breach may be intentional or unintentional.
• Breaches may harm the individual and damage the reputations of the Institute, the Researcher, and/or the staff involved.
• Breaches weaken the trust of the public and our study participants, affecting their willingness to participate in research.
• Corrective action requires time and money, for example, each individual with data breached must be notified.
Respecting Privacy, Safeguarding Data, Enabling Trust

This picture shows examples of privacy breaches.
Reporting a Privacy Breach

• There is a legal obligation to report a suspected or known breach of privacy

• Report to the Director of Quality and/or your Manager

• The TOH policy contains sanctions outlining disciplinary actions for privacy breaches. These sanctions have been posted along with these training slides and must be reviewed.

• The process for managing a reported breach is detailed in a “Privacy Breach Decision Tree” included in the Policy.

• Breaches must be reported by UOHI to the Office of the IPC and/or your professional body, if applicable

• Main goal is to learn and prevent a recurrence!
Preventing a Breach

**Do:**
- Access only info you require, limit access only to those who need it
- Log off when you are finished with your computer
- Store PHI only on a UOHI secure network drive and password protect the document
- Use UOHI encrypted device
- Separate PHI from research records ASAP, store in locked cabinets/offices
- Shred papers with PHI when no longer required
- Stay informed/continuing education, eg: CITI Canada Privacy course [https://www.citiprogram.org/index.cfm?region=7](https://www.citiprogram.org/index.cfm?region=7)

**Do Not:**
- Discuss confidential info in public areas
- Share passwords, except for shared documents within a study team
- Leave PHI unattended where it can be viewed by unauthorized users, including an open computer terminal
- Store PHI on personal C drive or mobile devices
- Surf information for your friends or family
- Contact patients without their expressed consent
- Release documents (ie: CRFs, logs) containing personal identifiers
Please respect the trust your study participant places in you …..not only for his/her care and safety, but also for his/her protection of privacy!

Our patients’ privacy is in your hands. Stop, think and protect before you act.
Contact Information

If you have any questions please contact Sharon Finlay, Clinical Research Manager at SFinlay@ottawaheart.ca.