UNIVERSITY OF OTTAWA
HEART INSTITUTE
INSTITUT DE CARDIOLOGIE
DE L'UNIVERSITÉ D'OTTAWA

Privacy Mandatory Training

Protect Privacy: It's the law!

2025

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

Protect Privacy: PHIPA, Ontario's Health Privacy Law

- PHIPA is the Personal Health Information Protection Act, 2004
- It **protects** the **privacy** of an individual, the **confidentiality** of an individual's personal health information (PHI), and, it gives individuals right of access to their health records. An individual can also request a correction of their health records.

- PHI is identifying information about an individual that related to:
    - Individuals physical or mental health, including family health history
    - The provision of health care to the individual, including the identification of the health-care providers
    - Or eligibility for health care, or eligibility for coverage for healthcare
    - Donation of body parts or bodily substances
    - Health card numbers (OHIP, RAMQ), medical record number
    - Identification of the individual's substitute decision maker (SDM)

- PHIPA sets the rules for **collection, use** and **disclosure** of PHI
- **Viewing** PHI is considered a form of "collection" and or "use"

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

Protect Privacy: PHIPA, Ontario's Health Privacy Law

Protecting Privacy: It's the law, it's the right thing to do, and it is your professional obligation.

- PHIPA applies to the Health Information Custodians (HICs) that collect, use and disclose personal health information (PHI).

Health Information Custodian (HIC):

- The Ottawa Hospital (TOH) is a "HIC" under the law and is accountable for the PHI it collects, uses and discloses.

Agents:

- Any person who is authorized by a HIC to perform services or activities in respect of PHI on the HIC's behalf and for the purposes of that HIC.
- As an agent, you need to obtain the patients consent for the collection, use or disclosure of PHI. Under (PHIPA) consent must:
  - Be knowledeable (i.e. the patient understands the purpose for the collection, use or disclosure and knows that they can give or withhold consent)
  - Relate to the information that will be collected, used or disclosed.
  - Not be obtained through deception or coercion

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

What is Express Consent?

Express consent is given either verbally or in writing, to collect, use or disclose PHI. It is also possible to expressly withhold or refuse to give consent to the collection, use or disclosure of PHI. If consent is withheld or not given, then you cannot collect, use or disclose PHI, unless PHIPA otherwise allows the practice without consent.

Implied consent is understood to be consent that the agent concludes has been given based on what the patient does or does not do in the circumstances. For example, when a patient walks into an Emergency Department and tells the Triage Nurse that they are having trouble breathing.

For assumed implied consent, you may assume that all the elements of consent are fulfilled. Assumed implied consent may only occur in the context of the “Circle of Care.” Unless the patient has specifically withheld or withdrawn their consent, you may assume their implied consent for providing health care within the “Circle of Care.”

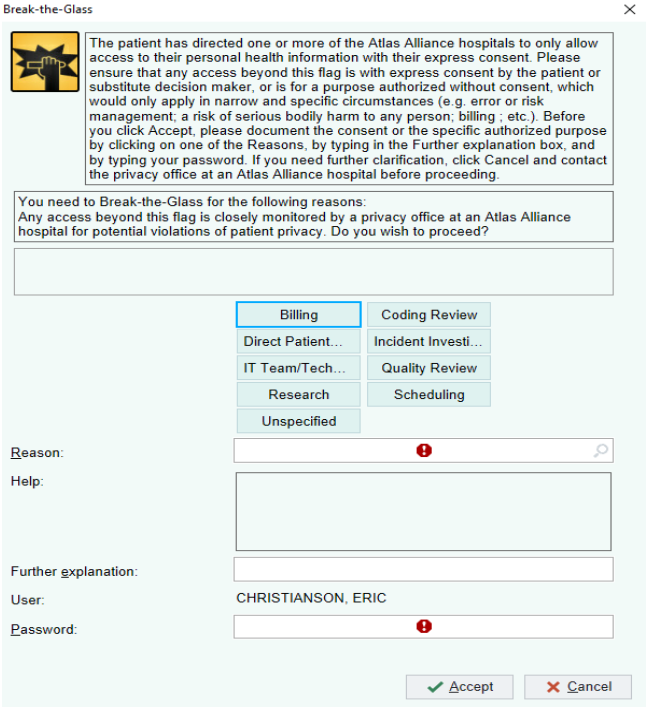
UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

Consent Directive & Break The Glass

- When a patient does not want their PHI shared with their other health care providers – it is called a lockbox request .
- Patients have the right to make choices about their personal health information.
- One way that patients can exercise this choice is to ask to use a "lockbox" to:

  Hide clinical information from health care providers at HIC (Restricted Use)
- Contact the UOHI Privacy Officer to add a consent directive or to remove a consent directive.

Please note when you are breaking the glass, the username and password is your Epic log in



UNIVERSITY OF OTTAWA
HEART INSTITUTE
INSTITUT DE CARDIOLOGIE
DE L'UNIVERSITÉ D'OTTAWA

Scenarios When You Can Break the Glass

When you have patients consent and the personal health information is required for health care purposes.

To prevent harm to the individual and you cannot obtain consent in a timely manner.

To prevent harm to others and you cannot obtain consent in a timely manner.

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

eHealth Ontario – Shared Electronic Health Record Systems

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

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

Similarities and Differences

eHealth Ontario's shared electronic health record systems are authorized for the purpose of:

- **Direct care** only
- Collecting/using/disclosing PHI for **any other** purpose will constitute a privacy breach

TOH's health records systems, including EPIC, are authorized for the purpose of:

- Direct care
- Hospital administration
- Approved research
- Quality assurance
- Prevention programs and early disease detection
- Fundraising (with the appropriate authority)

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

Physical, Administrative and Technical Safeguards

TOH, UOHI, OHRI and **eHealth Ontario** all use **safeguards** to protect PHI against loss/theft, unauthorized access, disclosure, copying, use or modification.

Physical Safeguards	Administrative Safeguards	Technical Safeguards
Locked filing cabinets Locked offices with restricted access Keeping electronic devices like iPads and laptops in secure location PHI backed-up and stored in a secure data centre	• Signed agreements to protect PHI • Awareness and training • Policies and procedures • Privacy Impact and Threat Risk Assessments • Privacy and Information Security Committee • Privacy and Security Attestations	• Auditing and monitoring systems to detect unauthorized access • Use Strong password or passphrase • Firewalls • Encryption • Lock and/or Log Off the computer when left unattended • Powering Off when not in use • Break-the-Glass Pop-Up • Clinical Viewer users who work for more than one organization must select TOH when acting on TOH's behalf • Search controls (open-ended searches are not allowed)

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

For safe and secure use of USB keys, paper documents, etc, 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?
- Acceptable solutions for cloud storage include Microsoft SharePoint and OneDrive. Third party solutions such as DropBox are not acceptable.

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

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

Electronic Communication

Email Messages between TOH/UOHI Staff:

- No PHI in subject line
- Use a private or confidential flag
- Use outlook encryption when sending external e-mails TOH/UOHI

E-mail Messages to Patients:

- Direct patient to access information by registering for MyChart
- Confirm the type of information they wish to receive (appointment reminders, financial billing information, etc.)
- Obtain and document consent to communicate by e-mail (this is not a secure platform unless using Outlook Encryption)

EPIC Messaging & MS Teams

- EPIC Messaging is the core clinical messaging app
- MS teams may be leveraged with Epic Messaging is unavailable or inefficiency, and may be used for exchanging PI/PHI
- See the Corporate SOP: Secure Transfer of Sensitive Information for details
- See Information Security's SharePoint site for details

UNIVERSITY OF OTTAWA
HEART INSTITUTE
INSTITUT DE CARDIOLOGIE
DE L'UNIVERSITÉ D'OTTAWA

Protect Privacy

- FIPPA is the Freedom of Information and Privacy Protection Act.
- The Act has two parts: (1) rights for the public to access information and (2) obligations for TOH to protect personal information.
- FIPPA is distinct from PHIPA. FIPPA allows for access to records that do not contain PHI.
- The public can access records (with some exceptions) through a Freedom of Information (FOI) request.
  - Records include emails, electronic files, databases, drafts, working notes, expense claims, agendas, meeting minutes.
- Follow the Retention and Destruction Policy.

Always assume that any record created could be disclosed and could enter the public domain.

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

Protect Privacy

What you should DO:

- Access only info you require
- Keep your passwords to yourself
- Log off when you are finished with your computer
- Store PHI on network
- Shred papers with PHI when no longer required
- Use UOHI encrypted mobile devices
- PHI leaving UOHI must be stored on encrypted mobile devices and password protected

What you CAN'T DO:

- Discuss confidential info in public areas
- Leave PHI unattended where it can be viewed by unauthorized users
- Surf information for your friends or family
- Leave a computer terminal with PHI readily visible to others
- Store PHI on unencrypted devices
- Share passwords

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

Your role in a suspected or actual Privacy Breach or Information Security Incident

REPORT

- Immediately notify your manager and the Information and Privacy Office at your local institution
- Complete a Privacy Incident report in the Safety Learning System (SLS).

CONTAIN

- Take reasonable and safe measures to contain the privacy breach or information security incident. (e.g. change your password if you suspect someone has used your login.)
- Log off a computer that you see logged in and unattended.
- Retain the evidence (e.g. a misdirected fax, etc.) as it will assist in the investigation and may be needed to contact the involved individuals.

COOPERATE

- Be prepared to cooperate in an investigation, as required.
- Assist with any remediation activities.

Human Error

Inadvertent action: Slip, lapse, or mistake

Ex. A misdirected fax or email

Manage through changes in:

- Processes
- Procedures
- Training
- Design
- Environment

At-Risk Behaviour

A Choice: Risk not recognized or believed insignificant or justified

Ex. Intentionally disclosing PHI through social media

Manage through:

- Removing incentives for at-risk behaviours
- Creating incentives for healthy behaviours
- Increasing situational awareness

Reckless Behaviour

Conscious disregard of substantial and unjustifiable risk

Ex. Snooping on family members, friends, or colleagues for personal gain or to cause harm

Manage through:

- Remedial action
- Disciplinary action

CONSOLE → **COACH** → **DISCIPLINE**

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

If you decide to breach privacy, it will cost you:

- Your position, your career and your reputation
- Review by your professional regulatory college
- Review by the Information and Privacy Commissioner of Ontario (IPC)
- Up to $200,000 in personal fines or up to one year in prison, or both
- A civil lawsuit and or prosecution*
- Retraining on privacy and security requirements
- Loss of access to one or more systems
- Significant financial and reputational losses for your organization
- As of January 1, 2024, the IPC has the discretion to issue administrative monetary penalties (AMPs) as part of its enforcement powers for violations of the Personal Health Information Protection Act (PHIPA). Penalties are up to a maximum of $50,000 for individuals and $500,000 for organizations.

***PHIPA requires that patients 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 cause the privacy breach.**

UNIVERSITY OF OTTAWA HEART INSTITUTE
INSTITUT DE CARDIOLOGIE DE L'UNIVERSITÉ D'OTTAWA

Acknowledgement and Confidentiality

Acknowledgement and Confidentiality Agreement

The University of Ottawa Heart Institute, the Ottawa Heart Institute Research Corporation, and the University of Ottawa Heart Institute Foundation (collectively, the "Institute") is committed to protecting the privacy and confidentiality of all personal information to which it is entrusted and the security of its facilities and personnel in order to carry out its mission.

This AGREEMENT applies to all persons providing services to the Institute. Security and systems access is conditional upon continued compliance.

I, , in consideration of my provision of services for, on behalf of, or for the benefit of the Institute ("Work"), understand and agree to comply with the following security and confidentiality requirements given that I will have access to secure locations of the Institute, confidential information, and/or personal health information:

- I understand there are legal obligations, under the *Personal Health Information and Protection Act 2004 (PHIPA)*, to maintain the confidentiality of all personal health information (PHI) whether collected for patient care or for research or quality purposes.
- I acknowledge that I have read, understand, and hereby agree to comply with The Ottawa Hospital (TOH) privacy policy (TOH Privacy – ADM II 260b) and UOHI Privacy Policy 1-200.
- I acknowledge that in the performance of my duties, I may have access to PHI, and that it is my obligation to maintain the security and confidentiality of all PHI.
- I acknowledge that I am prohibited from accessing PHI unless authorized by PHIPA to complete my Work including (but not

limited to) patient care, peer review, quality improvement, risk management, clinical research, or education.

- I understand that I may have access to confidential information, such as information that is of a confidential/proprietary nature or which is not a matter of public record, and that I must exercise discretion when discussing Institute business.
- I will not disclose, disseminate, or discuss confidential information and/or PHI except to other persons authorized to receive such information, and if doing so I will always do so by secure means.
- I will not alter, destroy, copy or interfere with any confidential information and/or PHI, except as authorized and expressly permitted.
- I acknowledge that the Institute has put in place security measures to safeguard confidential information and PHI, and that I am responsible for reviewing all policies made available on the Institute intranet (HeartHub) and TOH intranet (The Ottawa Hospital Policy and Procedure System (TOHPPS)) on an annual basis to ensure continued compliance.
- I acknowledge that user and computer system activities are monitored to protect patient privacy and comply with cybersecurity best practices.
- I will keep all access credentials (e.g., system account usernames/passwords) and access devices (e.g., UOHI-issued computers or smartphones) confidential and secure. I will not disclose my access credentials or lend my work-issued devices to anyone, nor will I attempt to use those of others. I will immediately change my access credentials if I believe they have been compromised.
- I will not share my assigned door keys or access card (employee ID card) with others and will keep these in a secure location when not on my person.
- When required for my Work, I will store PHI, sensitive/strategic information, and intellectual property on Institute-issued encrypted devices, Institute secure file shares such as (but not limited to) UOHI OneDrive and UOHI SharePoint locations, or Institute-issued USB memory sticks.

  I will not store or download such information on personal devices including (but not limited to) non-Institute-issued laptop computers or smartphones, on non-Institute-approved sites such as a "cloud" or "Dropbox", or on non-Institute-issued USB memory sticks or other recordable media.

- I will securely return all property of the hospital including but not limited to keys, access badge, and records of PHI at the conclusion of my employment or contractual relationship.
- I will notify my manager and the UOHI Privacy Office by phone or email at the first reasonable opportunity if I believe that a privacy breach or a breach of privacy policies may have occurred.
- I acknowledge and accept that the Institute will conduct random audits to ensure that PHI is not used or disclosed without proper consent.
- I will complete all assigned mandatory privacy and cybersecurity awareness training, and acknowledge that I have a duty to promptly report all potential cyber incidents to the UOHI IT Service Desk immediately. Cyber incidents may include (but not be limited to) user credential exposure, unauthorized access, inappropriate use of information systems, loss or corruption of data, abnormal application behavior, suspicious contact, or unauthorized interactions on social media platforms.

I agree and understand that failure to comply with this Agreement may result in suspension or termination of my privileges, termination of my employment or affiliation with the Institute, legal action, reporting to professional bodies, or penalties as stipulated by applicable law.

By signing this Agreement, I further acknowledge that my obligations as set forth herein will continue to remain in effect following the termination of my employment or affiliation with the Institute. A faxed, scanned, or other electronic copy of this Agreement shall be deemed as an original.

Legal Name: _____

Name: _____

Signature: _____ **Date** (dd/mm/yy): _____