



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

Privacy Mandatory Training

Protect Privacy: It's the law!

2024

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:
 - The Payment individuals physical or mental health, including family health history
 - The provision of health care to the individual, including the identification of the health-care provider
 - s 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"

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 patient's consent for the collection, use or disclosure of PHI. Under (PHIPA) consent must:
 - Be knowledgeable (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

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.”

Consent Directive & Break The Glass Pop UP

- 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.

Please note: when you are breaking the glass, the user and password is your EPIC log in

Break-the-Glass ×



The patient has directed one or more of the Atlas Alliance hospitals to only allow access to their personal health information with their express consent. Please ensure that any access beyond this flag is with express consent by the patient or substitute decision maker, or is for a purpose authorized without consent, which would only apply in narrow and specific circumstances (e.g. error or risk management, a risk of serious bodily harm to any person; billing ; etc.). Before you click Accept, please document the consent or the specific authorized purpose by clicking on one of the Reasons, by typing in the Further explanation box, and by typing your password. If you need further clarification, click Cancel and contact the privacy office at an Atlas Alliance hospital before proceeding.

You need to Break-the-Glass for the following reasons:
Any access beyond this flag is closely monitored by a privacy office at an Atlas Alliance hospital for potential violations of patient privacy. Do you wish to proceed?

Billing	Coding Review
Direct Patient...	Incident Investi...
IT Team/Tech...	Quality Review
Research	Scheduling
Unspecified	

Reason:

Help:

Further explanation:

User: CHRISTIANSON, ERIC


Password:

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 are not able to obtain consent in a timely manner.



To prevent harm to others and you are not able to obtain consent in a timely manner.

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)

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
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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)

Creating a Strong Password

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

To create a strong password that is easy to remember but difficult to guess:

1. Start with your favorite movie, food, clothing store, etc.
 - Example: **Large pizza, double cheese**
2. Combine the words in your phrase
 - Example: **largepizzadoublecheese**
3. Mix it up to get a strong passphrase. Use your imagination.
 - Example: **lgpizza2xcheese** or **LGpizza++cheez**

For more tips and tricks, see [Guidelines for creating secure passphrases](#)

CAUTION: Never use personal information in your passphrase. Your logon password must be a minimum of 12 characters.

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

Electronic Communication

Email Messages between TOH/UOHI Staff:

- No PHI in subject line
- Use a private or confidential flag
- Use Fortimail when sending external to 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 Fortimail)

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

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.

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

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

CONSOLE



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

COACH



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

DISCIPLINE

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 and the possibility of imprisonment
- 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.**

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 is it entrusted and the security of its facilities and personnel in order to carry out its mission.

The AGREEMENT applies to all persons providing services to the Institute/The Ottawa Hospital(TOH).

- 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's (TOH's) Privacy Policy (No. 00175, formerly Admin II – 260) and HI Privacy Policy 1-200.
- I acknowledge that in the performance of my duties, I may have access to PHI of patients at the Institute and it is my obligation to maintain the 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 will not disclose, disseminate or discuss confidential information and/or PHI except to other persons authorized to receive such information and by secure means.
- I will not alter, destroy, copy or interfere with any confidential information and/or PHI, except as authorized and expressly permitted