

1. ENGLISH

1.1 PROTECT PRIVACY:

PROTECT PRIVACY:
It's the law!

Mandatory Training
2020

 The Ottawa Hospital | L'Hôpital d'Ottawa

Inspired by research. Driven by compassion. **Inspiré par recherche. Guidé par la compassion.**

1.2 Protect Privacy:

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 the right of **access** to their health records, as well as, to request a **correction** of their health records.
- PHI is identifying information about an individual that relates to:
 - The individual's physical or mental health, including family health history
 - The provision of health care to the individual, including the identification of the health-care provider
 - Payments or eligibility for health care, or eligibility for coverage for health care
 - Donation of body part or bodily substance
 - Health number (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."

1.3 Protect Privacy:

Protect Privacy:

It's the law, it's the right thing to do and it's your professional obligation

PHIPA applies to 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.

1.4 Protect Privacy:

Protect Privacy:

Consent and Consent Directive

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

1.5 Protect Privacy:

Protect Privacy:

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 the 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."

1.6 Protect Privacy:


Protect Privacy:

Consent Directive & Break-the-Glass Pop-Up

- A patient may request a **consent directive** be applied to their health record, to an encounter or to a specific user.
- Health care providers may not access the patient's record without **express consent**, unless it is an authorized access that does not require consent, i.e.:
 - Risk of serious bodily harm to any person
 - Error or risk management
 - Billing, coding, etc.
 - Where permitted or required by law (i.e. to document care to a patient, court order, duty to report, etc.)
- All access beyond the Pop-Up is flagged to the Information and Privacy Office

More Details

Break-the-Glass

 STOP! The patient has blocked some of their information. You may only proceed if:
1. You have asked the patient for permission, or
2. The patient is unable to provide permission and there is a risk of harm, or
3. You need the information for hospital operations or another purpose that does not require patient permission (not including healthcare).

If you proceed, your action will be reviewed by the privacy officer at your hospital and an inappropriate override can lead to discipline including job loss and reporting to the Ontario's Information and Privacy Commissioner or your regulatory college.

You need to Break-the-Glass for the following reasons:
User needs to break the glass for appropriate access
Do you wish to proceed?

Reason	Billing	Coding Review	Direct Patient Care
	Incident Investigation	IT Team/Technical	Quality Review
	Research	Scheduling	Unspecified

1. **Ask** for the patient's consent (if required)
2. **Select** the appropriate "Reason" for requiring access (e.g. Billing, Direct Patient Care, Scheduling, Quality Review, etc.)
3. **Document** in the "Further explanation" box whether the consent was:
 - ✓ verbal or written, and
 - ✓ from patient or SDM
4. **Enter** your usual Microsoft password
5. **Click "Accept"**

Untitled Layer 1 (Slide Layer)

Protect Privacy:

Consent Directive & Break-the-Glass Pop-Up


In the **Ontario Laboratory Information System (OLIS)** an override to prevent harm is not permitted; rather, a block may only be overridden in OLIS with express consent by the patient or Substitute Decision Maker.

In the **Digital Health Drug Repository (DHDR)** users must obtain a "wet signature" before overriding a consent directive to the DHDR portal.

person

- Error or risk management
- Billing, coding, etc.
- Where permitted or required by law (i.e. to document care to a patient, court order, duty to report, etc.)
- All access beyond the Pop-Up is flagged to the Information and Privacy Office

Break-the-Glass

 STOP! The patient has blocked some of their information. You may only proceed if:


1. You have asked the patient for permission; or
2. The patient is unable to provide permission and there is a risk of harm; or
3. You need the information for hospital operations or another purpose that does not require patient permission (not including healthcare).

If you proceed, your action will be reviewed by the privacy officer at your hospital and an inappropriate override can lead to discipline including job loss and reporting to the Ontario's Information and Privacy Commissioner or your regulatory college.

You need to Break-the-Glass for the following reasons:
User needs to break the glass for appropriate access
Do you wish to proceed?

Reason	Billing	Coding Review	Direct Patient Care
	Incident Investigation	IT Team/Technical	Quality Review
	Research	Scheduling	Unspecified

1. **Ask** for the patient's consent (if required)
2. **Select** the appropriate "Reason" for requiring access (e.g. Billing, Direct Patient Care, Scheduling, Quality Review, etc.)
3. **Document** in the "Further explanation" box whether the consent was:
 - ✓ verbal or written, and
 - ✓ from patient or **SDM**
4. **Enter** your usual Microsoft password
5. **Click** "Accept"



1.7 Protect Privacy:

Protect Privacy:

eHealth Ontario - Shared Electronic Health Record Systems

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

- ConnectingOntario:** 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

1.8 Protect Privacy:

Protect Privacy:

eHealth Ontario and TOH's health record systems

Similarities and Differences

<p>eHealth Ontario's shared electronic health record systems are authorized for the purpose of:</p> <ul style="list-style-type: none">• Direct care only• Collecting/using/disclosing PHI for any other purpose will constitute a privacy breach	<p>TOH's health records systems, including EPIC, are authorized for the purpose of:</p> <ul style="list-style-type: none">• Direct care• Hospital administration• Approved research• Quality assurance• Prevention programs and early disease detection• Fundraising (with the appropriate authority)
--	---

1.9 Protect Privacy:

Protect Privacy:

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)

[**Click here to learn how to create secure passwords**](#)

Untitled Layer 1 (Slide Layer)

Protect Privacy:

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.

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.

1.10 Protect Privacy

Protect Privacy:

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

If any mobile device is lost or stolen, immediately report it to the HelpDesk (613-761-HELP)

1.11 Electronic Communication

Electronic Communication

Email Messages between TOH Staff:

- No PHI in subject line – use of MRN is permitted but not patient name or initials
- Use a private or confidential flag
- Encrypt and password protect attachments with PHI when sending external to TOH

Email Messages to Patients:

- Direct patients 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 email

See the Corporate SOP: Secure Transfer of Sensitive Information for details

EPIC Messaging & MS Teams

- EPIC Messaging is the core clinical messaging app.
- MS Teams may be leveraged when Epic Messaging is unavailable or inefficient, and may be used for exchanging PI/PHI

See Information Security's SharePoint site for details

1.12 Protect Privacy

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.

1.13 Protect Privacy:

Protect Privacy


Do use your TOH email for TOH business


Don't forget that emails may be requested under Freedom of Information (FOI) requests

Do recognize and report "phishing attacks"

Do follow the TOH policy for taking photos and videos for patient care

Do encrypt PHI if you must email it outside TOH

Do delete emails containing sensitive information as per the Retention and Destruction Policy

Don't auto-forward your TOH email to another account

Don't open attachments unless you know the source

Don't take photos or videos of patients or PHI

Don't share any PHI on Social Media such as Facebook, Twitter, etc.

Don't use your TOH email for non-TOH business

1.14 Phishing


Phishing

- Phishing is a method of gathering personal or payment information using deceptive e-mails and websites. The goal is to trick the recipient into clicking on a link or download an attachment.
- There are many cues that are used to help you spot a phishing email
- If you receive a phishing email:

Do investigate. Contact the senders using a phone number you know is real. <i>Verify authenticity.</i>	Don't trust organizations that send emails from an address like @gmail.com or @yahoo.com
Do report it. Forward the email to phishing@toh.ca	Don't click on links or attachments in the email.
Do delete the email if you suspect deception. <i>When in doubt, throw it out.</i>	Don't give out any personal or payment information.

1.15 How to spot a Phishing email

How to spot a Phishing email



- Non-personalized greetings.
- Alternate spellings (e.g. jsmith@tohh.ca or www.ottawahospital.ca).
- Email signatures that do not include contact information.
- Unexpected, and out-of-character, emails from people you know.
- Requests to verify accounts, credit card numbers, or reset passwords.
- Requests from senior executives to wire money or transfer funds.
- Threats to suspend accounts or incur a penalty/fine.
- Phishing emails often offer things for free such as *coupons*.

Untitled Layer 1 (Slide Layer)

Sample phishing email

xjdjyvksws-hackernet@gmail.com hovering over the sender's name with your mouse reveals the true sender's address

From: Susan Bertrand
Sent: April 10, 2019 3:50 PM
To: Kevin Roberts<kroberts@toh.ca>
Subject: Vendor Payment ISG-232

the sender claims to be a hospital employee but external mail banner appears indicating a non-TOH email address

CAUTION: External Mail. Do not click on links or open attachments you do not trust.
ATTENTION: Courriel externe. Ne cliquez pas sur des liens et n'ouvrez pas de pièces jointes auxquels vous ne faites pas confiance.

Hello Kevin,

Please ensure you wire an amount of \$37, 500 USD before the end of business day. My VP will be away on business to meet with the vendor next week. Our payment will be late and we may be asked to pay penalty fees if we don't wire the money today.

threat of a penalty or fine.

This email is unusual and out of character. Requests to transfer large sums of money are not made by email.

Susan Bertrand,
Executive Assistant to VP of Sales & Marketing
Phone: 613-798-5555, extension 54321

1.16 Protect Privacy:

Protect Privacy:

Privacy Breaches and Information Security Incidents

<p>Privacy Breach</p> <ul style="list-style-type: none">• A violation of:<ul style="list-style-type: none">• PHIPA• Privacy agreement(s)• Privacy policies, procedures and/or practices• Lost, stolen, unauthorized access of PHI• Unauthorized copying, modifying or disposal of PHI	<p>Information Security (IS) Incident</p> <ul style="list-style-type: none">• A violation or imminent threat of violation of Information Security (IS):<ul style="list-style-type: none">• Policies• Procedures• practices• IS event that may compromise operations, threaten the security of PHI and/or related business processes.
--	--

1.17 Protect Privacy:

Protect Privacy:

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

REPORT	CONTAIN	COOPERATE
<ul style="list-style-type: none">• 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).	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• Be prepared to cooperate in an investigation, as required.• Assist with any remediation activities.

1.18 Protect Privacy:

Protect Privacy:

Corrective Actions and Just Culture

<p><u>Human Error</u></p> <p>Inadvertent action: Slip, lapse, or mistake Ex. A misdirected fax or email</p> <p>Manage through changes in:</p> <ul style="list-style-type: none">• Processes• Procedures• Training• Design• Environment	<p><u>At-Risk Behaviour</u></p> <p>A Choice: Risk not recognized or believed insignificant or justified Ex. Intentionally disclosing PHI through social media</p> <p>Manage through:</p> <ul style="list-style-type: none">• Removing incentives for at-risk behaviours• Creating incentives for healthy behaviours• Increasing situational awareness	<p><u>Reckless Behaviour</u></p> <p>Conscious disregard of substantial and unjustifiable risk Ex. Snooping on family members, friends, or colleagues for personal gain or to cause harm</p> <p>Manage through:</p> <ul style="list-style-type: none">• Remedial action• Disciplinary action
--	---	--

Console → **Coach** → **Discipline**

1.19 Protect Privacy:

Protect Privacy:

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

- Your position, career and reputation
- Review by your professional regulatory college
- Review by the Information and Privacy Commissioner of Ontario
- 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

***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 caused the privacy breach.**

1.20 Acknowledgement of Confidentiality

Acknowledgement of Confidentiality

At The Ottawa Hospital (“TOH” or the “Hospital”) and our affiliated institutions, we are committed to protecting the confidentiality and security of all personal health information (“PHI”) of our patients, confidential information (“CI”) and personal information (“PI”) with which we are entrusted. The PHI and PI over which TOH has stewardship is subject to legislation including the *Personal Health Information Protection Act, 2004* (“PHIPA”), the *Freedom of Information and Protection of Privacy Act* (“FIPPA”), as well as TOH policies and procedures.

I understand and acknowledge that in the course of my employment or affiliation with TOH, I may be provided with access to CI, PHI or PI, or such information may be disclosed to me. In order to protect the confidential nature of such information and in consideration of the entering into and/or the continuance of my employment or affiliation with TOH, the Ottawa Hospital Research Institute (“OHRI”) and the University of Ottawa Heart Institute (“UOHI”), I understand and agree to the following:



Untitled Layer 1 (Slide Layer)

Acknowledgement of Confidentiality

At The Ottawa Hospital (“TOH” or the “Hospital”) and our affiliated institutions, we are committed to protecting the confidentiality and security of all personal health information (“PHI”) of our patients, confidential information (“CI”) and personal information (“PI”) with which we are entrusted. The PHI and PI over which TOH has stewardship is subject to legislation including the *Personal Health Information Protection Act, 2004* (“PHIPA”), the *Freedom of Information and Protection of Privacy Act* (“FIPPA”), as well as TOH policies and procedures.

I understand and acknowledge that in the course of my employment or affiliation with TOH, I may be provided with access to CI, PHI or PI, or such information may be disclosed to me. In

Click the checkbox below to agree. Completion of this module is considered to be full agreement with the Acknowledgement of Confidentiality.

understand and agree to the following:



1.21 Completed

Congratulations! You have completed this elearning module. Click the **green checkmark** below to exit.



2. FRENCH

2.1 PROTECT PRIVACY:

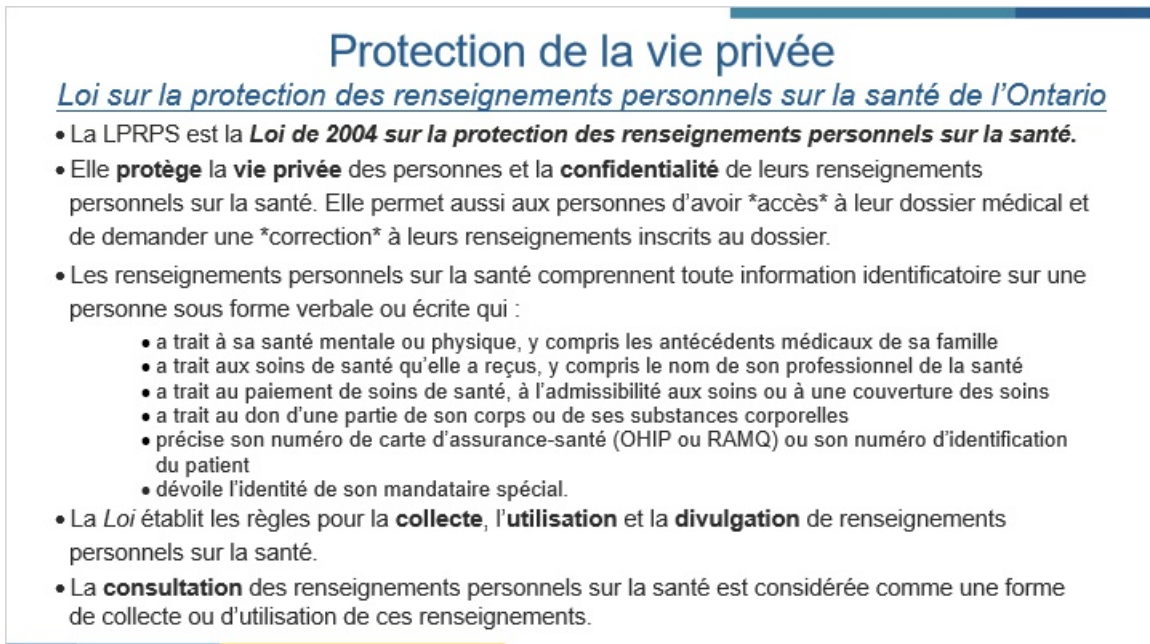


2020: Protection des renseignements personnels et sécurité de l'information

The Ottawa Hospital | L'Hôpital d'Ottawa

Inspired by research. Driven by compassion. Inspiré par recherche. Guidé par la compassion.

2.2 Protect Privacy:



Protection de la vie privée

Loi sur la protection des renseignements personnels sur la santé de l'Ontario

- La LPRPS est la **Loi de 2004 sur la protection des renseignements personnels sur la santé**.
- Elle **protège** la **vie privée** des personnes et la **confidentialité** de leurs renseignements personnels sur la santé. Elle permet aussi aux personnes d'avoir ***accès*** à leur dossier médical et de demander une ***correction*** à leurs renseignements inscrits au dossier.
- Les renseignements personnels sur la santé comprennent toute information identificatoire sur une personne sous forme verbale ou écrite qui :
 - a trait à sa santé mentale ou physique, y compris les antécédents médicaux de sa famille
 - a trait aux soins de santé qu'elle a reçus, y compris le nom de son professionnel de la santé
 - a trait au paiement de soins de santé, à l'admissibilité aux soins ou à une couverture des soins
 - a trait au don d'une partie de son corps ou de ses substances corporelles
 - précise son numéro de carte d'assurance-santé (OHIP ou RAMQ) ou son numéro d'identification du patient
 - dévoile l'identité de son mandataire spécial.
- La **Loi** établit les règles pour la **collecte**, l'**utilisation** et la **divulgation** de renseignements personnels sur la santé.
- La **consultation** des renseignements personnels sur la santé est considérée comme une forme de collecte ou d'utilisation de ces renseignements.

2.3 Protect Privacy:

Protection de la vie privée

C'est la loi, c'est la bonne chose à faire et c'est votre obligation professionnelle.

La *Loi* s'applique à tout dépositaire de renseignements sur la santé qui recueille, utilise et divulgue des renseignements personnels sur la santé.

Dépositaire de renseignements sur la santé

- L'Hôpital est **dépositaire de renseignements sur la santé** en vertu de la loi et est responsable des renseignements qu'il recueille, utilise et divulgue.

Mandataires

- Les professionnels de la santé à L'Hôpital d'Ottawa sont des *mandataires* en vertu de la loi et sont tous responsables de protéger les renseignements personnels sur la santé. À titre de membre du personnel de l'Hôpital et d'utilisateur de son système de dossiers de santé électroniques, d'**Epic**, et des systèmes de mise en commun de cyberSanté Ontario, vous devez rendre compte à l'Hôpital de vos actions concernant les renseignements personnels sur la santé.

2.4 Protect Privacy:

Protection de la vie privée

Consentement et directive de consentement

À titre de mandataire, vous devez obtenir le consentement du patient pour recueillir, utiliser ou divulguer ses renseignements personnels sur la santé. En vertu de la *Loi*, le consentement :

- doit être éclairé (c'est-à-dire que le patient comprend les fins visées par la collecte, l'utilisation ou la divulgation et sait qu'il peut refuser d'y consentir);
- doit porter sur les renseignements qui seront recueillis, utilisés ou divulgués;
- ne doit pas être obtenu par supercherie ni par coercition.

2.5 Protect Privacy:

Protection de la vie privée Qu'est-ce que le consentement explicite?

Le **consentement explicite** pour recueillir, utiliser ou divulguer des renseignements personnels sur la santé se donne verbalement ou par écrit. Il est aussi possible d'expressément interdire la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé. Si le patient refuse de donner son consentement ou le retire, vous ne pouvez pas recueillir, utiliser, ni divulguer ses renseignements personnels sur la santé, à moins que la *Loi* vous l'autorise sans l'obtention d'un consentement.

Le **consentement implicite** est une autorisation qui n'est pas obtenue directement. Le mandataire peut conclure par inférence qu'il a le consentement implicite du patient en raison des propos ou du comportement du patient dans les circonstances. Par exemple, si un patient se présente à l'Urgence en exprimant qu'il a de la difficulté à respirer, son comportement constitue un consentement implicite à la consultation de son dossier médical.

Dans le contexte du cercle de soins du patient, il est possible de **présumer le consentement implicite** du patient si tous les éléments du consentement sont respectés. Sauf si le patient a expressément refusé ou retiré son consentement, on peut présumer son consentement implicite à recevoir des soins des membres de son cercle de soins.

2.6 Protect Privacy:


Protect Privacy:

Consent Directive & Break-the-Glass Pop-Up

- Un patient peut demander de faire appliquer une directive sur le consentement pour « verrouiller » l'accès à son dossier médical par toute personne ou par certaines personnes en particulier.
- Dans un tel cas, un professionnel de la santé ne peut pas avoir accès au dossier médical du patient sans son consentement explicite, sauf dans les cas suivants :
 - prévention d'un préjudice (blessure) grave à une personne quelconque
 - gestion des risques et des erreurs
 - facturation, consignation, etc.
 - cas permis ou exigé par la loi (c.-à-d. consignation des soins au dossier du patient, ordonnance d'un tribunal, obligation de signaler, etc.).
- Tout accès au-delà de la fenêtre contextuelle est signalé au Bureau de la protection de la vie privée et de l'information.

Plus de détails

Break-the-Glass

 STOP! The patient has blocked some of their information. You may only proceed if:
1. You have asked the patient for permission, or
2. The patient is unable to provide permission and there is a risk of harm, or
3. You need the information for hospital operations or another purpose that does not require patient permission (not including healthcare).
If you proceed, your action will be reviewed by the privacy officer at your hospital and an inappropriate override can lead to discipline including job loss and reporting to the Ontario's Information and Privacy Commissioner or your regulatory college.

You need to Break-the-Glass for the following reasons:
User needs to break the glass for appropriate access
Do you wish to proceed?

Reason
Billing
Coding Review
Direct Patient Care
Incident Investigation
IT Team/Technical
Quality Review
Research
Scheduling
Unspecified

1. **Ask** for the patient's consent (if required)
2. **Select** the appropriate "Reason" for requiring access (e.g. Billing, Direct Patient Care, Scheduling, Quality Review, etc.)
3. **Document** in the "Further explanation" box whether the consent was:
 - ✓ verbal or written, and
 - ✓ from patient or SDM
4. **Enter** your usual Microsoft password
5. **Click "Accept"**

Untitled Layer 1 (Slide Layer)

Protect Privacy:


Dans le **Système d'information de laboratoire de l'Ontario (SILO)**, le contournement d'une restriction pour prévenir un préjudice n'est pas permis. Une restriction peut uniquement être contournée avec le consentement explicite du patient ou de son mandataire spécial.

Dans le **Répertoire numérique des médicaments (RNM)**, il faut obtenir une signature manuscrite avant de déroger à une directive sur le consentement.

- prévention d'un préjudice (blessure) grave a une personne quelconque
- gestion des risques et des erreurs
- facturation, consignation, etc.
- cas permis ou exigé par la loi (c.-à-d. consignation des soins au dossier du patient, ordonnance d'un tribunal, obligation de signaler, etc.).
- Tout accès au-delà de la fenêtre contextuelle est signalé au Bureau de la protection de la vie privée et de l'information.

← Moins de détails

Break-the-Glass

 STOP! The patient has blocked some of their information. You may only proceed if:
1. You have asked the patient for permission; or
2. The patient is unable to provide permission and there is a risk of harm; or
3. You need the information for hospital operations or another purpose that does not require patient permission (not including healthcare).

If you proceed, your action will be reviewed by the privacy officer at your hospital and an inappropriate override can lead to discipline including job loss and reporting to the Ontario's Information and Privacy Commissioner or your regulatory college.

You need to Break-the-Glass for the following reasons:
User needs to break the glass for appropriate access
Do you wish to proceed?

Reason	Billing	Coding Review	Direct Patient Care
Incident Investigation		IT Team/Technical	Quality Review
Research		Scheduling	Unspecified

1. **Ask** for the patient's consent (if required)
2. **Select** the appropriate "Reason" for requiring access (e.g. Billing, Direct Patient Care, Scheduling, Quality Review, etc.)
3. **Document** in the "Further explanation" box whether the consent was:
 - ✓ verbal or written, **and**
 - ✓ from patient or **SDM**
4. **Enter** your usual Microsoft password
5. **Click** "Accept"

2.7 Protect Privacy:

Protection de la vie privée

Systèmes de mise en commun de dossiers de santé électroniques de cyberSanté Ontario

Le système de dossiers de santé électroniques de **cyberSanté Ontario** comprend des outils qui permettent aux professionnels de la santé autorisés d'accéder à des renseignements personnels sur la santé, dont les suivants :

ConnexionOntario : rapports cliniques

Dépôt des services partagés en imagerie diagnostique : rapports d'examen en imagerie diagnostique

Système d'information de laboratoire de l'Ontario (SILO) : demandes et résultats d'analyses de laboratoire

Répertoire numérique des médicaments (RNM) : renseignements sur les médicaments et les services de pharmacie

2.8 Protect Privacy:

Protection de la vie privée

cyberSanté Ontario et les systèmes de dossier de santé de l'Hôpital

Similarités et différences

L'utilisation des systèmes de mise en commun de dossiers de santé électroniques de **cyberSanté Ontario** est autorisée aux fins suivantes :

- **soins directs** seulement.
- La collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé contenus dans les systèmes de cyberSanté à **toute autre fin** constitue donc une atteinte à la vie privée.

L'utilisation des systèmes de dossier de santé de l'Hôpital, dont Epic, est autorisée aux fins suivantes :

- soins directs
- activités administratives de l'Hôpital
- recherche approuvée
- assurance de la qualité
- programmes de prévention ou de détection précoce
- collecte de fonds (avec l'approbation appropriée).

2.9 Protect Privacy:

Protection de la vie privée

Dispositifs de protection physiques, techniques et administratifs

L'Hôpital d'Ottawa, l'Institut de cardiologie de l'Université d'Ottawa, l'Institut de recherche de l'Hôpital d'Ottawa et cyberSanté Ontario prennent plusieurs **mesures pour protéger** les renseignements personnels sur la santé contre la perte et le vol, ainsi que contre l'accès, la divulgation, la reproduction, l'utilisation et la modification non autorisés.

Mesures de protection physiques	Mesures de protection administratives	Mesures de protection techniques
<ul style="list-style-type: none">• verrouillage des classeurs• verrouillage des bureaux et restriction de l'accès• conservation des iPad et des ordinateurs portables en lieu sécurisé• entreposage et copie de sauvegarde des renseignements personnels sur la santé dans une base de données sécurisée.	<ul style="list-style-type: none">• signature d'ententes pour protéger les renseignements personnels sur la santé• sensibilisation et formation• politiques et procédures• évaluations des répercussions sur la vie privée, ainsi que des menaces et des risques liés à la vie privée• Comité de la protection des renseignements personnels et de la sécurité de l'information attestations de protection des renseignements personnels et de sécurité.	<ul style="list-style-type: none">• vérification et surveillance des systèmes en vue de déceler tout accès non autorisé• exigences pour la création de mots de passe forts• pare-feux• chiffrement• obligation de verrouiller l'ordinateur ou de fermer la session avant de s'absenter• mise à l'arrêt de l'ordinateur lorsqu'il n'est pas utilisé• fenêtre contextuelle « Break-the-Glass »• obligation à tout utilisateur du visionneur de ConnexionOntario qui travaille pour plus d'un organisme de sélectionner l'Hôpital lorsqu'il agit au nom de l'Hôpital• restriction des recherches (recherche ouverte impossible).

Comment créer un mot de passe sécurisé

Untitled Layer 1 (Slide Layer)

Protection de la vie privée

Dispositifs de protection physiques, techniques et administratifs

Pour créer un mot de passe fort et facile à retenir, mais difficile à deviner :

1. Inspirez-vous d'abord de votre film, aliment ou magasin préféré, par exemple.

- **Exemple** : Grande pizza double fromage

2. Combinez les mots en une seule expression - votre « phrase passe ».

- **Exemple** : grandepizzadoublefromage

3. Modifiez l'expression en y ajoutant des chiffres et des symboles. Faites preuve d'imagination.

- **Exemple** : grpizza2xfromage ou GRpizza++from

Pour plus d'astuces et de conseils, consultez les Lignes directrices pour la création d'une phrase passe sécuritaire.

Attention : N'utilisez jamais de renseignements personnels dans votre phrase passe. Remarque : Votre phrase passe doit contenir au moins 12 caractères.

2.10 Protect Privacy

Protection de la vie privée

Afin de veiller à la protection des données, notamment sur clé USB et en format papier, suivez la consigne suivante : **Arrêtez, pensez, protégez.**

ARRÊTEZ

Demandez-vous :

- *Dois-je absolument sauvegarder des renseignements personnels sur la santé sur cet appareil?*

Aux possibilités suivantes :

- Puis-je crypter les renseignements ou les rendre anonymes?
- Pourrais-je plutôt accéder aux renseignements à distance au moyen d'une connexion sécurisée ou d'un réseau virtuel privé?
- Solutions acceptables pour stockage infonuagique, notamment : Microsoft SharePoint et OneDrive. Les solutions de tierces parties, comme DropBox, sont interdites.

PENSEZ

PROTÉGEZ

Tout renseignement personnel que vous devez absolument sauvegarder sur un appareil mobile :

- Assurez-vous que les données sont bien cryptées.
- Sécurisez l'accès en utilisant un mot de passe fort.
- Assurez-vous de vérifier régulièrement si votre clé USB est exempte de virus

Si votre appareil mobile est perdu ou volé, signalez-le immédiatement au service d'assistance informatique (613-761-4357).

2.11 Electronic Communication

Communication électronique

Message transmis entre employés de l'Hôpital :

- N'inscrivez aucun renseignement personnel sur la santé dans l'objet du courriel – il est permis d'utiliser le numéro d'identification du patient, mais pas le nom ou les initiales du patient.
- Utilisez la mention « Privé » ou « Confidentiel » dans l'objet du courriel.
- Cryptez et protégez par un mot de passe les pièces jointes contenant des renseignements personnels sur la santé si le courriel est envoyé à l'extérieur de l'Hôpital.

Message transmis à un patient :

- Encouragez le patient à s'inscrire à MyChart pour y consulter son dossier.
- Confirmez le type de renseignements sensibles qu'il souhaite recevoir par courriel (p. ex. rappel de rendez-vous, renseignements sur la facturation).
- Obtenez et documentez le consentement du patient à la communication par courriel.

Pour en savoir plus, consultez la procédure opérationnelle normalisée de l'Hôpital sur le transfert sécuritaire d'information délicate.

Messagerie d'Epic et MS Teams

- La messagerie d'Epic est la principale application clinique de messagerie.
- MS Teams peut être utilisé quand la messagerie d'Epic n'est pas disponible ou inefficace pour communiquer des renseignements personnels et des renseignements personnels sur la santé.

Pour en savoir plus, consultez le site SharePoint de la Sécurité de l'information.

2.12 Protect Privacy

Protection de la vie privée

- La LAIPVP est la *Loi sur l'accès à l'information et la protection de la vie privée*.
- La *Loi* compte deux parties : 1) le droit d'accès à l'information par le public et 2) les obligations de l'Hôpital de protéger les renseignements personnels.
- La LAIPVP est différente de la *Loi sur la protection des renseignements personnels sur la santé*, car elle vise l'accès à l'information qui ne contient pas de renseignements personnels sur la santé.
- Le public peut avoir accès à des documents de l'Hôpital (avec certaines exceptions) en faisant une demande d'accès à l'information.
 - Documents de L'Hôpital d'Ottawa pouvant faire l'objet d'une demande d'accès : courriels, fichiers électroniques, bases de données, ébauches, notes de travail, demandes de remboursement de dépenses, ordres du jour et procès-verbaux de réunions.
- Suivre la politique de l'Hôpital intitulée « Conservation et destruction des dossiers »

Souvenez-vous donc toujours que tout document que vous créez pourrait être divulgué et rendu public.

2.13 Protect Privacy:

Protection de la vie privée

À faire et à ne pas faire : sécurité des courriels, médias sociaux et photos

	
<p>Utilisez votre adresse de courriel de l'Hôpital pour les affaires de l'Hôpital.</p> <p>Reconnaissez et signalez toute tentative d'hameçonnage.</p> <p>Suivez la politique de l'Hôpital pour prendre des photos et des vidéos dans le cadre des soins aux patients.</p> <p>Cryptez les renseignements personnels sur la santé si vous devez les envoyer par courriel à l'externe.</p> <p>Supprimez tout courriel qui contient des renseignements sensibles conformément à la politique sur la conservation et la destruction de documents.</p>	<p>N'oubliez pas que les courriels peuvent faire l'objet d'une demande d'accès à l'information.</p> <p>Ne faites pas rediriger automatiquement vos courriels de l'Hôpital à une autre adresse.</p> <p>N'ouvrez pas les pièces jointes à moins de connaître l'expéditeur.</p> <p>Ne prenez pas de photos ou de vidéos de patients ou de renseignements personnels sur la santé.</p> <p>Ne discutez pas de renseignements personnels sur la santé dans des médias sociaux comme Facebook ou Twitter.</p> <p>N'utilisez pas votre adresse de courriel de l'Hôpital pour les affaires non liées à l'Hôpital.</p>

2.14 Phising


Hameçonnage

- L'hameçonnage est une méthode utilisée par des fraudeurs pour recueillir des renseignements personnels et financiers par l'entremise de courriels et de sites Web frauduleux. Ainsi, les fraudeurs souhaitent piéger les destinataires en les incitant à cliquer sur un lien ou à télécharger une pièce jointe.
- De nombreux indices vous permettent de déceler un courriel d'hameçonnage.
- Si vous recevez un courriel d'hameçonnage :

Faites votre enquête. Appelez l'expéditeur par téléphone pour vérifier l'authenticité du message.	Méfiez-vous des organismes qui envoient des courriels provenant d'adresses comme @gmail.com ou @yahoo.com.
Signalez tout courriel douteux. Faites suivre le courriel à phishing@lho.ca.	Ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe d'un courriel douteux.
Supprimez le courriel si vous soupçonnez une escroquerie.	Ne donnez aucun renseignement personnel ni d'information sur le paiement.

2.15 How to spot a Phishing email

Caractéristiques d'un courriel d'hameçonnage



cliquez par
exemple

- Salutation non personnalisée
- Orthographe similaire à la version authentique (p. ex. jsmith@llho.ca ou www.hopitalottawa.ca)
- Signature du courriel sans coordonnées
- Courriel inattendu ou inhabituel provenant d'une personne que vous connaissez
- Demande de vérification de compte, de numéro de carte de crédit ou de réinitialisation de mot de passe
- Demande d'un membre de la haute direction d'envoyer de l'argent ou de transférer des fonds
- Menace de suspendre un compte ou d'imposer une pénalité ou une amende
- Les courriels d'hameçonnage offrent souvent des choses gratuites, comme des coupons-rabais.

Untitled Layer 1 (Slide Layer)

Sample phishing email

From: Susan Bertrand
Sent: April 10, 2019 3:50 PM
To: Kevin Roberts <kroberts@toh.ca>
Subject: Vendor Payment ISG-232

CAUTION: External Mail. Do not click on links or open attachments you do not trust.
ATTENTION: Courriel externe. Ne cliquez pas sur des liens et n'ouvrez pas de pièces jointes auxquels vous ne faites pas confiance.

Hello Kevin,

Please ensure you wire an amount of \$37, 500 USD before the end of business day. My VP will be away on business to meet with the vendor next week. Our payment will be late and we may be asked to pay penalty fees if we don't wire the money today.

Susan Bertrand,
Executive Assistant to VP of Sales & Marketing
Phone: 613-798-5555, extension 54321

Passez le curseur sur le nom de l'expéditeur pour voir sa véritable adresse courriel.

L'expéditeur se présente comme étant un employé de l'Hôpital, mais vous voyez la bannière « Courriel externe », qui signale que l'adresse courriel de l'expéditeur n'est pas une adresse de l'Hôpital.

Menace d'une pénalité ou d'une amende

Le courriel est inhabituel et inattendu. Une demande de transférer une somme importante d'argent ne se fait jamais par courriel.

2.16 Protect Privacy:

Protection de la vie privée

Atteintes à la vie privée et incidents liés à la sécurité de l'information

<p>Atteinte à la vie privée</p> <ul style="list-style-type: none">• Une violation :<ul style="list-style-type: none">• de la <i>Loi sur la protection des renseignements personnels sur la santé</i>• d'une entente de protection des renseignements personnels• des politiques, des procédures ou des pratiques établies pour protéger les renseignements personnels.• Perte ou vol de renseignements personnels sur la santé ou leur accès non autorisé• Copie, modification ou destruction non autorisée des renseignements personnels sur la santé	<p>Incident lié à la sécurité de l'information</p> <ul style="list-style-type: none">• Violation ou menace imminente de violation d'une politique, d'une norme, d'une procédure ou d'une pratique liée à la sécurité de l'information.<ul style="list-style-type: none">• Politiques• Procédures• Pratiques• Situation qui peut compromettre les activités de l'Hôpital, menacer la sécurité des renseignements personnels sur la santé ou les processus administratifs connexes.
---	---

2.17 Protect Privacy:

Protection de la vie privée

Vos obligations en cas d'atteinte à la vie privée (réelle ou soupçonnée) ou d'incident lié à la sécurité de l'information

SIGNALEZ	LIMITEZ	COLLABOREZ
<ul style="list-style-type: none">• Avisez immédiatement votre gestionnaire et le Bureau de la protection de la vie privée et de l'information.• Remplissez un Rapport d'incident du personnel dans le système d'apprentissage sur la sécurité (SLS).	<ul style="list-style-type: none">• Prenez des mesures raisonnables et sécuritaires pour limiter l'atteinte à la vie privée. (p. ex. changez votre mot de passe si vous pensez que quelqu'un l'aurait subtilisé).• Fermez votre session avant de laisser votre ordinateur sans surveillance.• Conservez toute preuve (p. ex. télécopie envoyée au mauvais destinataire), car elle sera utile à l'enquête et pourrait être nécessaire pour communiquer avec les personnes concernées.	<ul style="list-style-type: none">• Soyez prêt à collaborer à une enquête, au besoin.• Contribuez à appliquer les mesures qui s'imposent.

2.18 Protect Privacy:

Protection de la vie privée

Mesures correctives et culture juste

<u>Erreur humaine</u>	<u>Comportement risqué</u>	<u>Comportement téméraire</u>
<p>Geste involontaire : oubli, écart, erreur</p> <p>Exemple : Vous avez envoyé une télécopie ou un courriel par erreur au mauvais destinataire.</p> <p>Le gestionnaire devra prendre des mesures correctives en apportant des changements dans :</p> <ul style="list-style-type: none">• les processus• les procédures• les formations• la conception• le milieu.	<p>Un choix : risque inaperçu, pris à la légère ou jugé justifié</p> <p>Exemple : Vous avez divulgué intentionnellement des renseignements personnels sur la santé d'un patient dans les médias sociaux.</p> <p>Le gestionnaire devra prendre les mesures suivantes :</p> <ul style="list-style-type: none">• Retirer tout avantage à adopter des comportements risqués.• Créer des mesures incitatives pour les comportements sains.• Favoriser la prise de conscience de la situation	<p>Faire fi consciemment d'un risque important et injustifiable.</p> <p>Exemple : Vous avez consulté les dossiers de votre famille, d'amis ou de collègues par intérêt personnel ou pour causer du tort.</p> <p>Le gestionnaire devra prendre les mesures suivantes :</p> <ul style="list-style-type: none">• mesures correctives• mesures disciplinaires.

Consoler → **Encadrer** → **Imposer des mesures disciplinaires**

2.19 Protect Privacy:

Protection de la vie privée

Une atteinte à la vie privée délibérée pourrait entraîner :

- la perte de votre emploi, de votre carrière et de votre réputation
- une enquête par votre ordre professionnel
- une enquête par le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario
- jusqu'à **200 000 \$** d'amendes
- une poursuite civile ou judiciaire
- l'obligation de suivre une nouvelle formation sur la protection et la sécurité des renseignements personnels
- la perte de votre accès à un ou plusieurs systèmes
- d'importantes pertes financières et de réputation pour votre employeur.

La Loi exige que les patients soient informés si leurs renseignements personnels sur la santé ont été perdus, volés ou consultés sans autorisation. L'information qu'on leur transmet peut inclure le nom du membre du personnel ou de toute autre personne ayant causé l'atteinte à la vie privée.

2.20 ENTENTE DE CONFIDENTIALITÉ

ENTENTE DE CONFIDENTIALITÉ

L'Hôpital d'Ottawa et ses établissements affiliés se sont engagés à protéger la confidentialité et la sécurité de tous les renseignements personnels sur la santé des patients et de tout autre renseignement confidentiel ou personnel qui leur sont confiés. Les renseignements personnels sur la santé et autres renseignements personnels que gère l'Hôpital sont soumis aux lois, dont la *Loi de 2004 sur la protection des renseignements personnels sur la santé (LPRPS)*, de la *Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP)* et des politiques et procédures de l'Hôpital.

Je comprends et atteste que dans le cadre de mon emploi ou de mon affiliation à l'Hôpital, je peux avoir accès à des renseignements personnels sur la santé ou autrement confidentiels ou personnels. Pour protéger la confidentialité de ces renseignements confidentiels et en vue de travailler, de continuer de travailler ou d'être affilié à L'Hôpital d'Ottawa, à l'Institut de recherche de l'Hôpital d'Ottawa (IRHO) ou à l'Institut de cardiologie de l'Université d'Ottawa (ICUO), je conviens de respecter les modalités suivantes :



Untitled Layer 1 (Slide Layer)

ENTENTE DE CONFIDENTIALITÉ

Cliquez sur la case ci-dessous pour accepter. L'achèvement de ce module est considéré comme un accord total avec ENTENTE DE CONFIDENTIALITÉ



2.21 Completed

Félicitations! Vous avez terminé ce module de formation en ligne. Cliquez sur le crochet vert ci-dessous pour quitter le module.

