Personal Health Information (PHIPA)
Freedom of Information & Protection of Privacy Acts (FIPPA) and how they affect us.

Leslie Lunstroth
Manager, Transcription, Health Records & Privacy Services
Privacy Officer

Overview

- Highlights of Ontario PHIPA and FIPPA Acts
- Privacy
  - Audits
  - Breach Management
  - Examples in the Media
- Video with examples of how we can slip into inappropriate disclosures of patient information and ways we can help each other to prevent this
- Review “Privacy Breach Management” and other privacy policies
- **Read the Confidentiality Agreement carefully before signing! You are responsible to know your obligations.**

OSMH Privacy Officer

- Reports directly to CEO on matters of Privacy
- Responds to patient requests to access and correct
- Ensures that all employees, volunteers, and others are informed of their legal duties under the acts
- Answer staff & patient questions about information practices
- Notified regarding inquiries and complaints about possible violations of the law
  - Including privacy concerns, privacy complaints
  - Conducts privacy audits
- Reports annual statistics on privacy, PHIPA and FIPPA to Ontario's Information and Privacy Commissioner (IPC)

PHIPA & FIPPA

- Protection of personal privacy is a key principle of both Acts.
- The privacy protection rules are based on two assumptions:
  1. An individual has the right to control his or her own personal information; and
  2. Rules governing the collection, use, disclosure, retention, security, and disposal of personal information are necessary to protect privacy.
- Culture of openness is encouraged so that information should be available to the public and that exemptions should be limited and specific.

FIPPA: Non patient related information requests

- Non patient related information requests must be directed to the hospital's FIPPA office.
- These requests could be for
  - **Personal Information:** protected and disclosed only as required
  - **General Records:** should be made widely available to support transparency and accountability
- Right of Access is to all records in the facility.
- Anything recorded, or that can be made into a record, whether in print, audio or electronic form is a record
  - Email, paper files, electronic files, video tapes, audiotapes, notebooks, sticky notes, handwritten notes etc.
- **So, create records with access in mind!**
  - ***What is recorded - could be on the front page one day***
- Records should be factual, objective and include only what is relevant

PHIPA: Consent

- Rely on implied consent in Health Care before we collect, use or disclose PHI
- Notices displayed at each Registration area
- Covers the concept of “Circle of Care” – the sharing of PHI for Health Care purposes
  - When a patient is being treated at OSMH, our physicians may access records of the GBIN partners. This is covered in the circle of care.
- Patient may request that they do not want specific information used
- Express consent required for other purposes

"Connecting Ontario" by eHealth – June 2018

- Some clinical and clerical staff will be given access to the Connecting Ontario portal.
- Information available includes PHI from contributing sites
  - DI reports & images, Dictations, Labs, etc.
- Same rules apply as Hospital EMR in terms of access, consequences for breaching privacy.
  - i.e. You may only view/handle patient's PHI in the portal if you are currently treating that patient.

Connecting Ontario
POWERED BY EHEALTH ONTARIO

PHIPA: Patients Accessing their Health Records

- Requests (oral or written)
- Can occur when patient is still receiving care
  - Attending physician/care provider consulted (to ensure access could not result in a risk of serious harm to patient or someone else)
  - Contact Health Records with any questions
- Safeguard the documents
  - Monitor the patient if he/she is viewing original documents
- After discharge, refer the patient to Health Records
- *No records from GBIN partner sites are to be released by any other site.*
- *No Connecting Ontario records are to be released – refer the patient to Health Records Release of Information.*

Process for Correcting Health Records

- You may respond to an oral request if the patient can show that the record is not correct or complete and gives you the information to correct it
- Only written requests invoke the rights and procedural requirements set out in the Act and should be referred to the Privacy Officer

Connecting Ontario:

- Refer Connecting Ontario errors to the Privacy Officer.

Types of Security

Physical Security

- Information left on counter, cart, desk, bedside
- Transfer – only copies (not originals) may leave facility
- Locked areas
- White boards
- Computer screens being visible
- Conversations held in hallways, public areas

- Who you see in the workplace is private – ask their permission to share any information
- Privacy Officer works with the managers to review physical areas for any potential problems and work together on solutions

Types of Security

Technological Security

Passwords, firewalls, disaster recovery, inventory of computer data and how it is secure.

- Audits are conducted on a regular basis of the computer system access.
  - Portion is random sample; and
  - Targeted for privacy flagged patients
  - May be conducted upon request or complaint
  - NEVER share your password!
  - NEVER leave your workstation unlocked!

- Auditing will deal with unauthorized access of patient records including VIP and staff records.

Types of Security

Administrative Security

- Confidentiality Agreements for all employees and agents (includes physicians, volunteers, students)
- Access restrictions
  - EMR has more capability to limit access
  - Connecting Ontario access is limited to those who need to know

Breaches

Breaches can occur in many ways, and can be accidental or purposeful:

- Loss (file is misplaced)
- Theft (a laptop or file is stolen)
- Mistake (letter faxed to the wrong person)
- Unauthorized or unsecured disposal
- Unauthorized collection of information
- Unauthorized access to PHI in the EMR
- Posting on social media such as Facebook, Instagram

- Caring & concern are never a valid reason to look up someone's records.
- You cannot access your own record, or those of your family.
- May only access to do your job at OSMH.
- Who you see here is private - Ask permission before sharing

Privacy Issues in the Media – Student on placement

"Clinton, ON –

- ***Student has been fined $20,000 plus a $5,000 victim surcharge*** for breaching the privacy of family health team patients in the Clinton area. It's the highest fine for such a case in Canada.
- The IPC says the ***student who was working on an educational placement*** pleaded guilty to the breach
- Commissioner Brian Beamish says it sends a message that snooping on medical records will not be tolerated." – *March 17, 2017*

Largest Health Fine Levied After Breach In Clinton Area

Regional | by Peter Jackson

Student charged $25,000, after accessing 139 patient files at Clinton-area health practice.

A student has been fined $20,000 plus a $5,000 victim surcharge for breaching the privacy of family health team patients in the Clinton area.

It's the highest fine for such a case in Canada.

The office of the Information and Privacy Commissioner says the student who was working on an educational placement pleaded guilty to the breach that happened between September 2014 and March 2015.

Privacy Issues in the Media

Pair at Princess Margaret Cancer Centre, who pleaded guilty**, are the first ever convicted** under Ontario's health privacy act. - By: May Warren, The Star – May 6, 2016

Two health workers who snooped into late mayor Rob Ford's electronic health records have become **the first in Ontario to be convicted** under the province's health privacy law, the Star has learned.

Mohammad Rahman, of Toronto, and Debbie Davison, of Pickering, both pleaded guilty under the Personal Health Information Protection Act (PHIPA) to "willfully collecting, using or disclosing personal health information," while working at the University Health Network (UHN) Princess Margaret Cancer Centre in January 2015.

Each was fined $2,505, according to court records.

Three hospital workers have been charged under Ontario's health privacy law for snooping into former mayor Rob Ford's medical records after he was diagnosed with cancer.
Court documents obtained by the Star show Caroline Goodridge, of Laurel Ave., Mohammad Rahman, of Massey Square and Debbie Davison, of Redbird Crescent, Pickering, all face charges under PHIPA.
The allegations include "willfully collecting, using or disclosing personal health information" at the University Health Network (UHN) Princess Margaret Cancer Centre in January... – Toronto Star July 8, 2015


Govt. prosecutes health workers for snooping into Rob Ford's medical records

Three Toronto hospital workers face prosecution for snooping into Rob Ford's records at the Princess Margaret Cancer Centre. If convicted, it will be the first successful health privacy prosecution in Ontario's history.

Tweet

TWITTER

Dan Jacobs, chief of staff to Councillor Rob Ford, tweeted this photo one morning in May morning as Ford prepared to undergo cancer surgery. Three hospital staffers have now been charged with snooping into Ford's medical records during his fight with cancer.


TV RADIO NEWS SPORTS MUSIC KIDS LOCAL MORE WATCH LISTEN LOG IN

CBCnews | Toronto

LIVE Toronto More Streams
Radio One
Listen Live

Home World Canada Politics Business Health Arts & Entertainment Technology & Science Trending Weather

Canada Toronto Photo Galleries

Rob Ford medical-records snoopers should be charged, privacy watchdog says

A conviction for looking at health records at University Health Network could result in $50K fine

CBC News Posted: Mar 25, 2015 11:38 AM ET | Last Updated: Mar 25, 2015 4:34 PM ET

hospital ORILLIA SOLDIERS' MEMORIAL

Excellent compassionate care...Every Day

Privacy Issues in the Media – Ophthalmologist Office

June 2016

CANADIAN Healthcare Technology

Transform your tom
with a complete patient reco

HOME EVENTS CURRENT ISSUE ARCHIVES ABOUT US LINKS ADVERTISE SUE

Class action suit launched against Trillium Health

June 22, 2016 0 Comment e-Messenger

TORONTO – A proposed class action for a breach of privacy has been commenced against Trillium Health Partners, Mississauga Ophthalmologist Dr. Tony Vettese, and his assistant, Lisa Lyons. The claim seeks $2 million in general damages as well as exemplary damages and punitive damages, plus individual awards for class members, costs and interest.

Mississauga businesswoman and Trillium patient Katie Mallinson has alleged that Lyons used her access to Trillium's entire database to secretly review the confidential medical records of Trillium patients for many years and hundreds of times.

The class action characterizes Lyons as an electronic "Peeping Tom," who surreptitiously looked into the private lives of her victims, for her own amusement. Neither Mallinson nor Class Members are current patients of Vettese

Ontario's Information & Privacy Commissioner

Hospital privacy violations rife in Ontario

More than 400 complaints about privacy breaches are lodged each year, yet only one

Privacy commissioner calls on health authority to fire employee who breached 880 patient files

Privacy commissioner intervening in Peterborough hospital privacy breach case

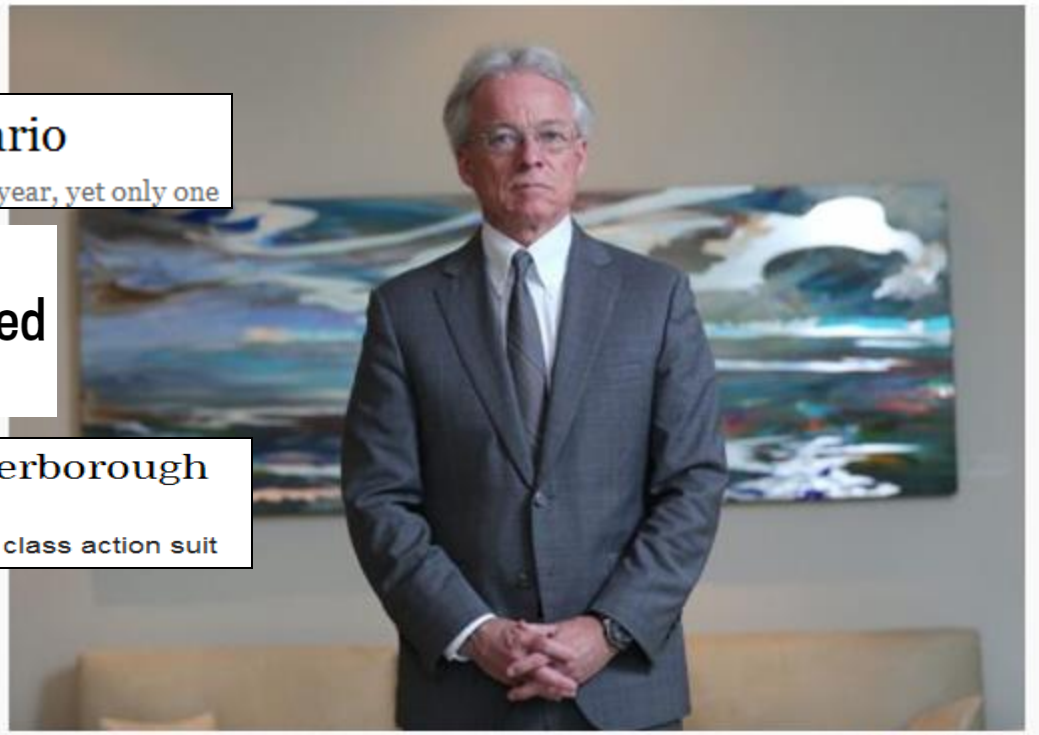
Commissioner to argue court has authority to hear $5.6 million class action suit

Island Health fires two over privacy violations

VICTORIA - Vancouver Island's health authority says it has fired two employees who looked at more than 100 patients' private healthcare records to satisfy their curiosity. Island Health says the employees looked at 112 electronic health records of patients with whom they had no care relationship. More ▸▸

Hospital staff have reportedly been fired after a privacy breach at Bluewater Health.

Multiple sources told The Observer Monday as many as 17 people were dismissed after non-clinical staff accessed patient information through a password-protected system — without authorization — earlier this month.



VINCE TALOTTA / TORONTO STAR Order this photo

Brian Beamish, Ontario's acting privacy commissioner, is calling for changes in legislation to make it harder for hospitals to handle privacy breaches internally without reporting them to the privacy office.

Hospital privacy breach 'unprecedented,' regulatory body says

It doesn't happen at OSMH… does it?

CANADIAN Healthcare Technology

Audit reveals snooping into patient charts

May 20, 2015 0 Comment e-Messenger

ORILLIA, Ont. – Three employees of Orillia Soldiers' Memorial Hospital are no longer working at the medical centre, while another employee is under further investigation, after they were caught snooping into the health records of over 50 patients over the past five years. All four privacy breaches were identified through routine hospital audits.

…gation into this matter, (the hospital) is confident …hospital spokesperson Terry Dyni told the Toronto …atient records.

Four hospital clerks caught snooping in patient files

Orillia Soldier's Memorial Hospital caught four employees peering into 52 patient records.

Theresa Boyle

Toronto Star

An Orillia hospital has caught four clerical employees peering into patient files.

What happens when it does?

OSMH staff snoops into records of friends, colleagues and neighbours out of curiosity - What happens?

- Computer access suspended/employee could be sent home.
- Investigation includes interview by Privacy Officer and Manager.
- Discipline up to and including termination.
- Notification:
  - Regulatory college informed, resulting in further discipline.
  - IPC Notified, investigates
  - Patients notified of the breach, including:
    - information accessed
    - what the hospital is doing to prevent future breaches
    - employee's name if requested

Consequences

- Employee faces embarrassment / reactions from those whose PHI was breached.
- IPC notified - may recommend to the Attorney General that a fine be charge under PHIPA against the:
  - employee *up to $100,000*
  - Hospital *up to $500,000*
- Patients may bring forward legal action.
- Could be front page news in the local media.
- Potential employment repercussions – reference.
- Damage control done by many people – CEO, Risk Management, Public Affairs, Privacy Office, Board.
- COST to OSMH is staggering

Be cautious of suspicious emails and links

- Hackers try to steal email lists from companies. Company email addresses are valuable to attackers, allowing them to create fake emails from “real people”
- Opening these emails or clicking on links in them can compromise your computer without you ever knowing it .
- In most cases hovering over the link will reveal it’s true source. Emails from government agencies or large organizations such as banks would never use a “@gmail” or “@hotmail” account

What to do with suspicious emails and links

- If you are unsure about a suspicious email – contact I.T. Help Desk @ ext. 3559
- Forward the message if you aren't sure if the email is legitimate

Cell phones

- No Texting of Personal Health Information
  - Texting of administrative information only
- Prohibits taking pictures of data
- Do not take pictures of patients or staff without permission

USBs

- Last resort only
- Ensure USB is encrypted!

Email Usage

- Prohibits use of personal email accounts to send/receive PHI to/from the EHR Solution Program Team or eHealth Ontario
- Encrypt emails that contain PHI, use a secure file transfer solution or a secure e-mail system (i.e. ONE mail)
- Emails containing PHI should not be sent to outside addresses unless authorized by Manager or Privacy Officer
- Prohibits personal emails being sent/received to/from your work email

So remember…

- Only collect, view, use or discuss patient information in the provision of Care or Services for the Patient.
- Do not post about patients (including pictures) on social media.
- "What happens here, stays here"
- Who you see here is private
  - Ask permission before sharing any information

For further information

Contact OSMH Privacy Officer:

Leslie Lunstroth

705-325-2201 ext. 3626

llunstroth@osmh.on.ca

Please be sure to sign the Confidentiality Agreement!