Association of Ontario Health Centres
Community-governed primary health care

aohc acso

Association des centres de santé de l'Ontario
Soins de santé primaires gérés par la communauté

Privacy in Healthcare or why you need to be even more careful in 2016?!



June 8, 2016

Simeon Kanev



The content of this presentation should not be considered a legal opinion. It is based on extensive research of materials available online and consultations with other privacy professionals. If you need a legal advice, please refer to your legal counsel.



Presenter Disclosure

Presenter: Simeon Kanev

Relationships to commercial interests:

Grants/Research Support:	None
Speakers Bureau/Honoraria:	None
Consulting Fees:	None
Other:	None

Topics for discussion

- Bill 119 – Health Information Protection Act (HIPA)
- Some IPC expectations
- Rise of ransomware in 2016
- Common privacy questions
- Summary

News

Privacy breach: Six GTA hospitals gave patient info to photographers

Mount Sinai, North York General, St. Joseph's, Humber River, Toronto East General and Rouge Valley gave patient info to baby photographers.

Tweet 99 g+1 3 reddit this!

14

Peterborough Regional Health Centre privacy victims file $5.6M lawsuit over employees snooping their medical records

News / GTA

Rouge Valley faces $400M class-action lawsuit over privacy breach

Rouge Valley Centenary is named as a defendant in a class-action lawsuit on behalf of ation was leaked by staffers.

POSTED TORONTO

TRENDING Ghomeshi | Ottawa | Magnotta | ISIS | Ford | NHL | Remembrance Day

Two staffers at Toronto hospital disciplined after 'inappropriately' viewing Rob Ford's medical records

Tristin Hopper | October 16, 2014 7:20 PM ET
More from Tristin Hopper | @TristinHopper

ddit this! + save to mystar

on Wed Jun 25 2014

been brought against a Scarborough hospital on personal information was leaked by two former

h that the contact information of as many as ary, mainly mothers who gave birth between

NEWS BRANTFORD-BRANT

Norfolk General Hospital notifies 1,300 o breach 25

DANIEL R. PEARCE & MONTE SONNENBERG
Wednesday, August 14, 2013 8:44:17 EDT AM

Seven PRHC jobs lost over privacy breaches 0

ELIZABETH BOWER and SARAH DEETH Examiner Staff Writers
Saturday, May 5, 2012 3:29:50 EDT AM

Local News

Breach of privacy leaves patient's family distraught

Saturday, May 03, 2014 *by:* Darren Taylor

A Sault Ste. Marie woman is

The Western Star > News > Local

Western Health privacy breach charge going to trial

Gary Kean
Published on November 29, 2013

Aug 27, 2014 | Vote 0 0

May 14, 2016 | Vote 0 0

Privacy breach at Joseph Brant Hospital leaves more questions than answers

The province is taking steps to better protect heath information, but it's tough to combat curiosity

More than 6,000 new mothers at Ajax-Pickering hospital may have had privacy breached

Names on contact information handed over to RESP companies

f the ial

ce

remain anonymous, has told SooToday.com a letter she received from Sonia Tassone, freedom of information and privacy coordinator at SAH, dated April 2, 2014, informs her that a March 31, 2014 audit of the hospital's MediTech system shows her mother's files were inappropriately accessed by an SAH employee.

How serious are convictions for privacy breaches?

Hospital clerk fined $36,000 for selling patient records

Shaida Bandali also sentenced to two years of probation after selling thousands of maternity patient records to RESP firms.

- $36,000 fine
- 2 years probation
- 300 hrs community service

- 3 months house arrest, a part of a 6 months conditional sentence
- 2 years probation
- 340 hrs community service

Hospital information schemers sentenced to house arrest

An RESP broker and former maternity ward nurse pleaded guilty Tuesday to their role in scheme to peddle RESPs to new parents.

Hospital workers convicted for snooping into Rob Ford's personal health files

Pair at Princess Margaret Cancer Centre, who pleaded guilty, are the first ever convicted under Ontario's health privacy act.

- First to be convicted under PHIPA
- Fined $2,505 each

- 4 months suspension
- Formal reprimand

North Bay nurse who snooped into 5,800 patients' records gets four month suspension

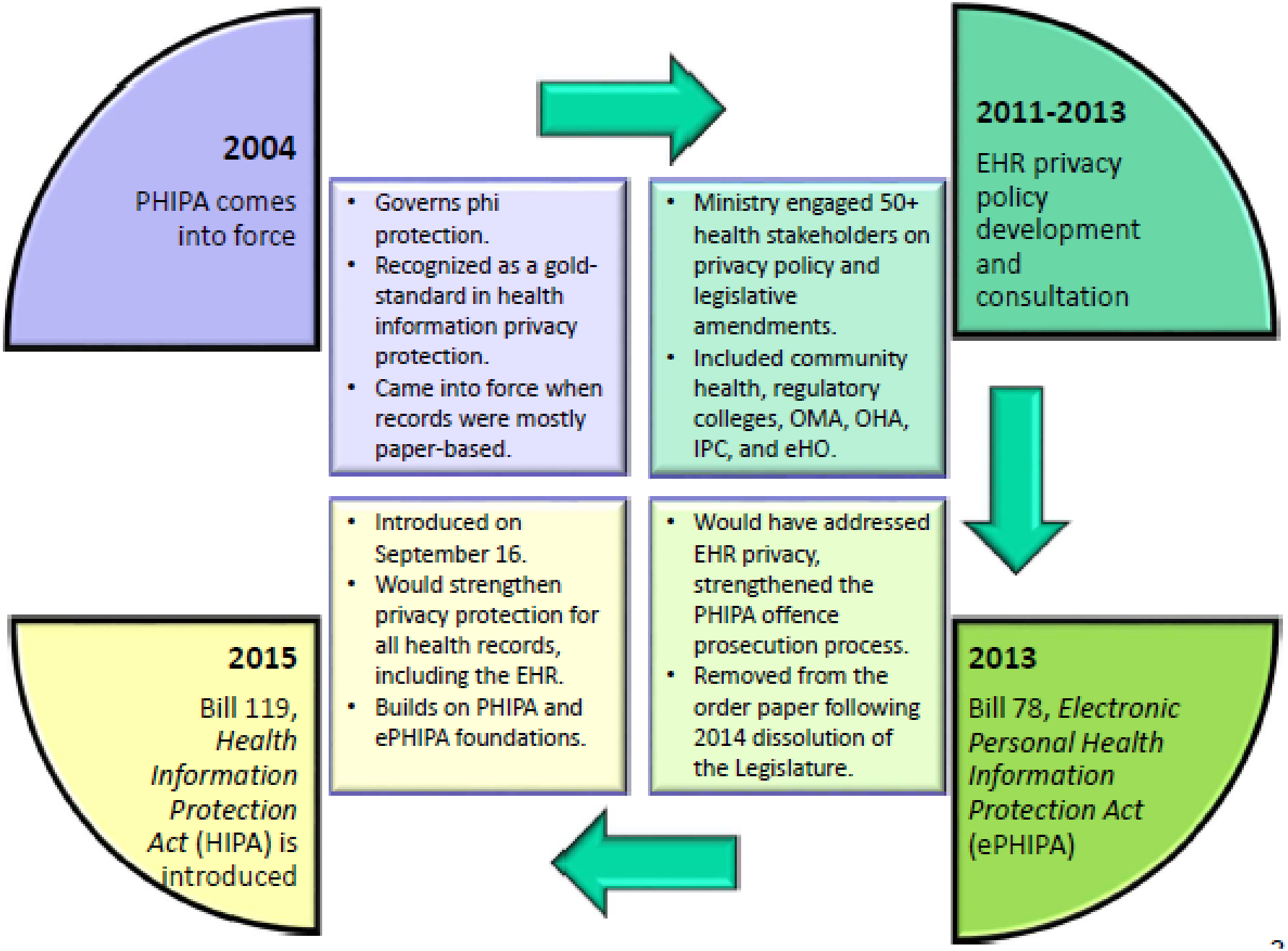
Melissa McLellan, the first person charged under Ontario's health privacy law, also received a formal reprimand from the College of Nurses of Ontario.

Highlights – Bill 119

- First reading – Sept 16, 2015
- Second reading – Feb 18, 2016
- Third reading – May 5, 2016
- Royal Assent - May 18, 2016

Bill 119 is now official and will come into effect once the accompanying regulations are approved which should happened most likely by the end of the year.

Health Information Privacy Legislation Development



Privacy Protection Amendments:

- Amend definition of “use” to explicitly include “viewing”
- Clarify “unauthorized activities” that constitute a breach
- Broaden breach notice and reporting requirements
- Clarify what agents are/are not permitted to do with PHI
- Require HICs to take steps to ensure agents comply with restrictions re: handling of PHI
- Clarify HICs continued responsibility for PHI mishandled by their agents
- Clarify IPC’s review role

Notable prosecution-related amendments:

Remove the 6 months limitation period for commencing a prosecution

Double the fines for conviction to a maximum of $100,000 for an individual and $500,000 for an organization

Some IPC expectations

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

- Paper-based records/printouts must be properly protected and securely disposed of when no longer needed (HO 1 & 6);
- Any PHI stored on a mobile device (USB drive, cell phone, tablet, laptop, etc.) must be encrypted with a strong password (HO 4, 7 & 8);
- Strong policies and procedures and discipline for those who snoop into records (HO 2, 10 & 13).

Some IPC expectations

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

- Annual confidentiality pledges (HO 13);
- Privacy training should be repeated on a yearly basis to include IPC/O videos, in-house or externally-facilitated privacy training (HO 13);
- Monthly random audits of EMR to monitor for privacy breaches and inappropriate access to patient records (HO 13);
- Flag (to the extent that it is possible) likely targets of inappropriate access by staff (such as family members of staff and high-profile individuals in the community);
- Privacy warning to the EMR record to pop up automatically upon log-in.

Why do I need to know all that?

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

- IPC is the overseeing entity in Ontario, in charge of enforcing PHIPA;
- Health orders bind the entities that have been named explicitly;
- Best practice for anyone else;
- Once mentioned in a HO, higher level of expectation re: compliance.

Strength in numbers







The rise of ransomware in 2016

- A type of malware that locks your files and demands ransom to unlock;
- Highly dangerous and very profitable;
- Targets everyone ;
- People and organizations pay the criminals to get back in control.
- How do you know that if you pay, your files are yours only? Have you heard of “extortionware”?

How to prevent: regular backups, patching and updating, training and awareness for staff.

Some common questions



- Am I allowed to leave a voice message for clients with health information?
- What do we do when staff are clients of our organization?
- Are we allowed to look at our own health records? What about our children's health records? Or as a favour to a friend?
- Can I look at a health record after care is provided if I'm concerned about the client but I'm no longer providing care?

Some very common questions (cont'd)



- Can we use email to communicate with clients/other health care providers? Text message? Skype?
- Should staff use client numbers instead of client names when calling into a waiting room?
- Is it a breach if someone overhears another person's health information (e.g., diagnosis)?
- What the heck is ransomware and should I be worried?

Some very common questions (cont'd)



- What do I do when a client comes up to me at the grocery store?
- What is the circle of care? Are we allowed to share information with the hospital? School? CAS? Police?
- Can I give health information in response to letters from lawyers, criminal investigations, insurance companies?
- What do I need to teach staff in terms of using shared systems?

Privacy Resources on Members' Portal

All materials have been approved by the Privacy Working Group (PWG) which consists mainly of member organizations' Privacy officers.

PRIVACY RESOURCES

Enter search criteria...

Group Home | Group Pages | Directory & Features | Options

Group Admin Options | Change Homepage Layout

Share |

Privacy Resources

This is your one-stop-shop for anything privacy-related. If you need any assistance, please email privacy@aohc.org.

What's new:



To access the Security Awareness Training module, please click the link below depending on the language you want to take the training:

Security Awareness training

Formation sur la sensibilité de la sécurité



To access the Privacy Training module, please click the link below depending on the language you want to take the training:

Privacy training

Formation sur la protection de la vie privée

ITEM NAME
Circle of Care summary PDF (266.57 KB)
Client Consent Toolkit Briefing Note - EN PDF (183.63 KB) [more]
Client Consent Toolkit Briefing Note - FR PDF (262 KB)
Consent and its 3 different kinds - summary PDF (40.04 KB)
Lessons Learnt from 2015 Data breaches PDF (215.04 KB)

Privacy AOHC - Policies, Procedures, Tools

ITEM NAME
DISCLAIMER - Read Me PDF (186.23 KB)
AOHC General Privacy Training PPTX (290.75 KB)
Client Consent Toolkit - EN PDF (244.59 KB)
Release of Information form DOCX (34.21 KB) [more]
Incident and Breach Management Toolkit PDF (366.42 KB)
Client Consent Toolkit - FR PDF (1017.58 KB)
Privacy Tips poster PDF (140.28 KB) [more]
Sample - Privacy Brochure for HICs DOC (89.5 KB) [more]
Sample Breach Notification Letter DOCX (15.11 KB) [more]
Privacy Auditing in Nightingale on Demand (NOD) DOCX (73.06 KB) [more]
Privacy Audit Work book XLSX (98.93 KB)
Privacy Lead Roles and Responsibilities DOCX (43.97 KB)
Sample Privacy Policy PDF (107.13 KB)

Summary / Take aways

- Privacy is becoming more and more important and the fines for breaches are now doubled;
- Education and awareness are key strategies to mitigate the risk;
- If something is considered Best Practice by IPC, you better take that at face value;
- Security and Privacy are the two sides of the same coin;
- If in doubt, ask.

Questions



privacy@aohc.org