IAPP CANADA
Privacy Symposium 2018

MANDATORY BREACH REPORTING: REVIEW OF THE REQUIREMENTS UNDER PHIPA

OVERVIEW OF BREACH NOTIFICATION AND IPC STATISTICS

- Fida Hindi, Legal Counsel

Office of the Information and Privacy Commissioner of Ontario

- This presentation is provided for educational purposes and is not legal advice

#CPS18

BREACH NOTIFICATION

- Pre-Existing:
  - A health information custodian must notify an affected individual at the first reasonable opportunity if personal health information in its custody or control is stolen, lost or used or disclosed without authority
- In addition:
  - A custodian must notify the IPC if the circumstances surrounding the theft, loss or unauthorized use or disclosure meet the **prescribed requirements**
  - A custodian must also, on or before March 1 in each year starting in 2019, provide the IPC with a statistical report of breaches in the previous calendar year

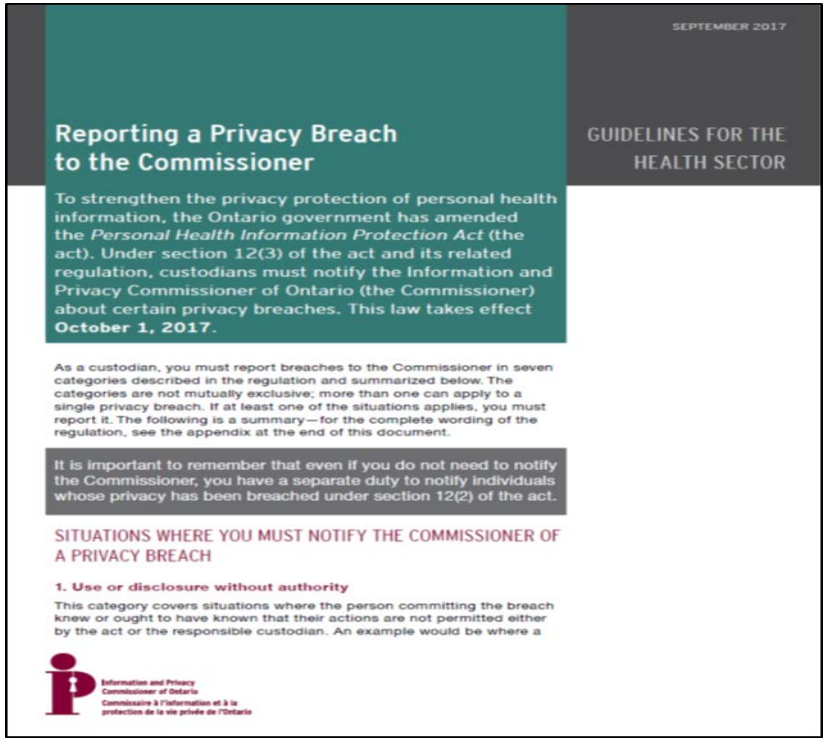
NOTIFICATION TO REGULATORY COLLEGES

- Custodian must provide written notice to regulatory College where a health care practitioner the custodian employs or that the custodian extends privileges to, or is otherwise affiliated with:
  - is terminated, suspended, subject to disciplinary action or member's privileges are revoked, suspended or restricted, or his or her affiliation is revoked, suspended or restricted, as a result of a breach
  - resigns or relinquishes/voluntarily restricts his or her privileges or his or her affiliation and custodian has reasonable grounds to believe that this is related to an investigation or other action by the custodian with respect to a breach

PRESCRIBED REQUIREMENTS

You must notify the IPC in cases of:

1. use or disclosure without authority
2. stolen information
3. further use or disclosure without authority after a breach
4. pattern of similar breaches
5. disciplinary action against a college member
6. disciplinary action against a non-college member
7. significant breach



SEPTEMBER 2017

GUIDELINES FOR THE HEALTH SECTOR

Reporting a Privacy Breach to the Commissioner

To strengthen the privacy protection of personal health information, the Ontario government has amended the *Personal Health Information Protection Act* (the act). Under section 12(3) of the act and its related regulation, custodians must notify the Information and Privacy Commissioner of Ontario (the Commissioner) about certain privacy breaches. This law takes effect **October 1, 2017.**

As a custodian, you must report breaches to the Commissioner in seven categories described in the regulation and summarized below. The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, you must report it. The following is a summary—for the complete wording of the regulation, see the appendix at the end of this document.

It is important to remember that even if you do not need to notify the Commissioner, you have a separate duty to notify individuals whose privacy has been breached under section 12(2) of the act.

SITUATIONS WHERE YOU MUST NOTIFY THE COMMISSIONER OF A PRIVACY BREACH

1. Use or disclosure without authority

This category covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. An example would be where a

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

#CPS18

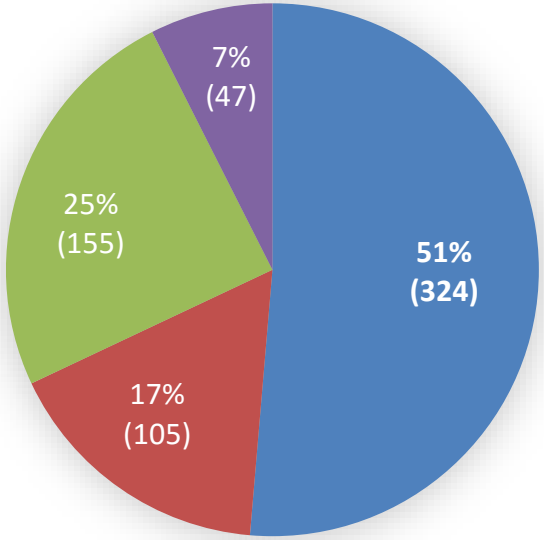
STATISTICS

	October 1, 2017-December 31, 2017	October 1, 2016-December 31, 2016
Total Breaches	125	58
Misdirected/Lost	36.7%	28%
Snooping	24%	24%
Unauthorized collection, use, disclosure	18.4%	15%
Stolen/Inadequately secured	20.9%	33%

The total number of breaches reported between October 1, 2017-December 31, 2017 represents a 115% increase over the same period in the previous year.

#CPS18

HEALTH SECTOR PRIVACY COMPLAINTS 2017



Self-Reported Breach
Collection-Use-Disclosure
Access/Correction
IPC Initiated

Of the 324 self-reported breaches:

- 60 snooping incidents
- 8 ransomware/cyberattack

Remaining 256 were:

- lost or stolen PHI
- misdirected PHI
- records not properly secured
- other collection, use and disclosure issues

#CPS18

SELF REPORTED BREACHES IN 2018

- 185 self-reported breaches in 2018:
  - 72 misdirected/lost PHI
  - 38 snooping incidents
  - 34 general collection, use and disclosure issues
  - 20 stolen PHI
  - 8 lost or stolen mobile devices
  - 8 records not properly secured
  - 4 ransomware/cyberattack

ANNUAL STATISTICAL REPORTS TO THE COMMISSIONER

- Custodians will be required to:
  - Start tracking privacy breach statistics as of January 1, 2018
  - Provide the Commissioner with an annual report of the previous calendar year's statistics, starting in March 2019

NOVEMBER 2017

Annual Reporting of Privacy Breach Statistics to the Commissioner

REQUIREMENTS FOR THE HEALTH SECTOR

Starting in March 2019 health information custodians will be required to provide the Commissioner with an annual report on privacy breaches occurring during the previous calendar year.

This requirement is found in section 6.4 of Ontario Regulation 329/04 made under to the *Personal Health Information Protection Act, 2004*, as follows:

(1) On or before March 1, in each year starting in 2019, a health information custodian shall provide the Commissioner with a report setting out the number of times in the previous calendar year that each of the following occurred:

1. Personal health information in the custodian's custody or control was stolen.
2. Personal health information in the custodian's custody or control was lost.
3. Personal health information in the custodian's custody or control was used without authority.
4. Personal health information in the custodian's custody or control was disclosed without authority.

(2) The report shall be transmitted to the Commissioner by the electronic means and format determined by the Commissioner.

For custodians to prepare for this reporting requirement, they must start tracking their privacy breach statistics as of January 1, 2018. The following is the information the IPC will require in the annual report.

#CPS18

THANK YOU

Office of the Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada M4W 1A8
Phone: (416) 326-3333 / 1-800-387-0073
TDD/TTY: 416-325-7539

Web: www.ipc.on.ca
E-mail: info@ipc.on.ca
Media: media@ipc.on.ca / 416-326-3965

#CPS18

PRACTICAL TOOLS FOR BREACH NOTIFICATION

- Natalie Comeau, CIPP/C, Manager, Privacy, FIPPA & Information Access

Providence St. Joseph's and St. Michael's Healthcare

- Mary Jane Dykeman, Partner

DDO Health Law

#CPS18

A HIC EXPERIENCE

- Providence Healthcare, St. Joseph's Health Centre and St. Michael's Hospital integrated into one network on August 1, 2017

THE PLAN

- Institutional template for IPC questions
- Process for review and escalation
- New log to track all breaches, including:
  - References to incident reporting systems
  - Institutional metrics (e.g. affected department, date of patient notification)
  - IPC metrics for annual report (e.g. PHIPA breach category)

THE JOURNEY INCLUDED…

- Defining (and re-defining) the organization's risk tolerance & risk categories
  - **Low** = few impacted patients, unintentional violation, minimally sensitive PHI, and no anticipated harm
  - **Medium** = many impacted patients, negligent or repeated violation, moderately sensitive PHI, or potential harm
  - **High** = large number of impacted patients, intentional violation, most sensitive PHI, or patient harmed (* or IPC involvement)

IT'S AN OPPORTUNITY TO…

- Socialize breach definitions and examples

Type	Notice/report required	Notice/report at the HIC's discretion	Policy/contractual violation
Theft	Theft of an unencrypted device containing PHI	Loss of an encrypted device containing PHI	Theft of PHI in the custody of another HIC
Unauthorized Use	Accessing a locked record without consent or a significant risk of harm	Sending a record of PHI in error to another agent (e.g. internal staff)	Individual accesses their own record directly (against hospital policy)
Unauthorized Disclosure	Sending a record of PHI to an unintended recipient that was opened, read or otherwise collected	PHI sent to the right provider at the wrong location	Temporary unsecure storage, without evidence of inappropriate access

LESSONS LEARNED

- Staff learned the right thing to do when learning about what can go wrong (& how to prevent common mistakes)
- Increased staff ownership & engagement
- No decrease in breach reporting
- Culture matters

PRIVACY OFFICER QUESTIONS

- Many privacy officers in Ontario wear multiple other hats in the health care organization
- Some do not have robust systems for tracking breaches
- Turnover in the role is very high in some organizations resulting in lost legacy

CAUTIONARY TALES

- Important to recognize the nuances IPC is providing as breach reporting matures
- Remember that even if not reportable to IPC, the duty under s. 12(2) of PHIPA to give notice to the affected individual remains (e.g. accidental breach)
- Issues in determining whether a breach is part of a pattern or was it accidental/ inadvertent?

PRACTICAL APPROACHES

- They are asking:
  - How do we make breach reporting seamless?
  - What are other organizations doing?
  - What templates are being used? (e.g., OHA)
  - What's the difference between mandatory breach to IPC and the annual statistical reporting?
    - Tracking as of January 1, 2018; reporting March 2019 and includes those breaches for which no mandatory report was made to IPC

THANK YOU

Natalie Comeau, CIPP/C, Manager, Privacy, FIPPA & Information Access – Providence Healthcare, St. Joseph's Health Centre & St. Michael's Hospital	416-557-9163 comeau@smh.ca
Mary Jane Dykeman, Partner - DDO Health Law	416-967-7100 ext. 225 mjdykeman@ddohealthlaw.com

#CPS18

HOW DID THINGS GO? (WE REALLY WANT TO KNOW)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

- Start by opening the IAPP Events App
- Select this session and tap “Rate the Session”
- Once you’ve answered all three questions, tap “Done” and you’re all set
- Thank you!

#CPS18