A PHIPA Update from the IPC

Sherry Liang
Assistant Commissioner, Tribunal Services
Information and Privacy Commissioner of Ontario
January 25, 2017

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

Themes

- *PHIPA* processes
- *PHIPA* decisions
- Unauthorized access
- Update on HO-013 (Rouge)
- Email Fact Sheet
- Bill 119

PHIPA Processes

- Internal review of *PHIPA* processes led to some changes
  - Most significant: an increase in the number of public decisions, in order to give public guidance and increase transparency
  - IPC now issues "*PHIPA* Decisions" which can include:
    - Orders
    - Decisions not to conduct a review
    - Decisions following a review, with no orders
    - Interim decisions
  - 25 Decisions and Interim Decisions issued since August 2015

PHIPA Processes – *cont'd.*

- Other changes as result of review:
  - More staff involved in *PHIPA* Decisions
    - PHIPA Orders previously written primarily by Commissioner or Assistant Commissioner
    - IPC Adjudicators and Investigators to write more decisions,
  - Code of Procedure for all *PHIPA* files being finalized, with additional Practice Directions
    - New or revised Practice Directions to deal with:
      - Litigation guardians
      - How to respond to access requests
      - IPC practice on naming HICs and respondents

PHIPA Processes – *cont'd.*

- Have not changed:
  - Efforts to reach early resolution of complaints
  - 70% of access/correction complaints and 60% of collection/use/disclosure complaints are settled
  - Additional number are screened out at an early stage without a review
- Almost all self-reported breaches are resolved at Intake

Some PHIPA Decisions

- Applying access provisions: *PHIPA* Decision 17
- What is a reasonable search in response to an access request: *PHIPA* Decision 18
- Can a complaint be made about a refusal to disclose: *PHIPA* Decisions 19, 20, 21, 22
- Approach to issuing an interim order: *PHIPA* Decision 23
- Decision not to conduct a review: *PHIPA* Decision 32
- Duty to correct health records: *PHIPA* Decision 36

Unauthorized access

- The IPC receives about 300-350 complaints about privacy breaches in the health sector per year.
- Most are caused by carelessness, such as the loss or theft of portable devices or misdirected emails or faxes.
- About 2 or 3 cases per month of intentional “snooping” into records of personal health information
- Very few snooping cases have resulted in orders - custodians (mainly hospitals) take them seriously and take steps to address IPC’s concerns about any systemic issues that have contributed to the snooping.

Goal of IPC Investigations

- Determine whether to refer to Attorney General for prosecution
- Determine whether response of health information custodian was adequate including:
  - Notice to affected patients
  - Disciplinary response
  - Addressing systemic issues
    - Auditing/logging
    - Training
    - Confidentiality agreements
    - Privacy warnings on electronic systems

Referrals to Prosecution

- It is an offence to wilfully collect, use or disclose personal health information in contravention of *PHIPA* or its regulations.
- IPC does not prosecute, but rather refers certain matters to the Attorney General.
- In deciding whether or not to refer a case to the AG, some of the factors the IPC considers are:
  - Were the actions "wilful", e.g:
    - recent privacy training
    - recently signed confidentiality agreement
    - ignoring privacy warnings on the system
  - Number of occurrences
  - Motive
  - Disciplinary action taken; complaint to professional college
  - Interests/views of the patient

Referrals to Prosecution - *cont'd.*

- To date, six individuals have been referred for prosecution:

  2011

  A nurse at the North Bay Health Centre

  2015

  Two radiation therapists at the University Health Network (Mayor Rob Ford)

  A social worker at a family health team

  A registration clerk at a regional hospital

  2016

  A regulated health professional at a Toronto hospital

Referrals to Prosecution – *cont'd.*

Outcome of referrals

- Case from 2011 dismissed for delay
- UHN case
  - two convictions; each individual fined $2000
- Registration clerk
  - 443 patients
  - Pled guilty; $10,000 fine, $2500 victim surcharge
- Family Health Team in small community
  - Trial pending
- Health professional at hospital
  - Referred to AG in 2016; no word on charges

Update on HO-013 (Rouge)

- ***PHIPA* Order HO-013**
  - An employee of the Rouge Valley Health System gathered information about new mothers and sold their contact information to RESP providers
  - IPC investigated and concluded that the hospital did not take reasonable steps to protect personal health information.
  - Several orders were made, one of which was that the hospital change its electronic information systems to ensure the ability to audit all instances of access to PHI

Update on HO-013 (Rouge) – *cont'd*.

- The hospital appealed HO-013 to the Divisional Court.
- After discussions between the hospital and the IPC, the hospital withdrew its appeal on the following basis:
  - The hospital and the IPC would cooperate on strategies to implement the Order provisions relating to its electronic information systems.
  - The IPC and the hospital would agree on a work plan setting out a time frame for the actions noted in the plan.
- Hospital and IPC have now agreed on the plan

Update on HO-013 (Rouge) – *cont'd*.

The Plan Going Forward

- The hospital identified electronic systems containing personal health information.
- The hospital will buy software that performs logging and auditing.
- The IPC and the hospital agreed on the systems that will be covered by the software.
- The software will not be deployed to systems, for example, that are due to retire soon, to which limited staff have access, or which only conduct real-time monitoring and do not record personal health information.
- A schedule was developed for deployment.

Communicating PHI by Email

- **Fact Sheet**
  - Issued in September
  - describes the risks of using email and custodians' obligations under PHIPA.
  - outlines some of the technical, physical and administrative safeguards needed to protect personal health information when communicating by email and the policies, procedures and training custodians should have in place.
- Fact Sheet distinguishes between custodian to custodian and custodian to patient communications
- For email between custodians, IPC expects encryption, barring exceptional circumstances

Communicating PHI by Email – *cont'd.*

- Email between custodians and patients
  - Use of encryption where feasible
  - Otherwise, consider risk-based approach
  - Approach to emailing patients should be captured in a policy
  - Consent of patients should be obtained
- Data minimization principle applies, even with patient consent
- Custodians have obligation to retain and dispose of emails containing PHI in a secure manner
- Only retain emails containing PHI as long as necessary to serve purpose; avoid duplication
- Encrypt portable devices

Bill 119 Amendments

- Amendments to *PHIPA* that have been proclaimed in force include the following:
  - Privacy breaches meeting a threshold must be reported to the IPC and to health regulatory colleges (in certain circumstances)
    - Threshold on reporting to IPC to be prescribed in regulation
  - Six month time limit on laying charges under *PHIPA* removed
  - Fines for offences under *PHIPA* doubled from $50,000 to $100,000 for individuals and $250,000 to $500, 000 for organizations.
  - Persons other than Attorney General may commence prosecution, with AG's consent

How to Contact Us

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