Privacy Breaches
Causes, Prevention, Response

David Goodis

Assistant Commissioner

Information and Privacy Commissioner of Ontario

Canadian Identity Theft Prevention Association
Identity Theft & Data Breach Conference
June 14, 2016

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

Our Office

- Ontario Information and Privacy Commissioner (IPC) provides **independent** review of government decisions and practices concerning access and privacy

- Commissioner is appointed by, reports to the Legislative Assembly

- Commissioner Brian Beamish
- 5 year appointment beginning 2015

IPC Legislation

- *Freedom of Information and Protection of Privacy Acts* ***FIPPA/MFIPPA***
  - Ontario public sector: ministries, agencies, hospitals, universities, municipalities, school boards
- *Personal Health Information Protection Act, 2004* ***PHIPA***
  - health information custodians (hospitals, labs, clinics, health professionals)
- in Ontario, *PIPEDA* applies to private sector

IPC Breach Reporting

- no mandatory breach reporting to IPC under *FIPPA/MFIPPA*
- mandatory breach reporting to IPC for health information when *PHIPA* amendments come into force (likely 2017)
- but we receive reports under all three statutes
  - 130 public sector self-reported (2015)
  - 175 health sector self-reported (2015)
  - more learned from complainants, media

Common Causes of Privacy Breaches

1. Insecure disposal of records
2. Lost/stolen portable devices
3. Unauthorized access (snooping)

Common Causes of Privacy Breaches

1. Insecure disposal
   - records intended for shredding are recycled
     - film shoot case (IPC Order HO-001)
   - improper destruction of electronic records
     - hard drives not wiped/destroyed
   - records abandoned when business transfer or termination
     - common in health sector (doctors, dentists)
     - PHIPA Decision 23 (2016)

Common Causes of Privacy Breaches

2. Lost/stolen portable devices
   - IPC Order HO-008 (2010)
     - hospital laptop stolen from employee's car
     - device not encrypted
   - IPC Elections Ontario Investigation (2012)
     - unencrypted USB key lost with voting PI of up to 2.4 million people

Common Causes of Privacy Breaches

3. Unauthorized access

- malware
  - e.g. ransomware that locks organization out of its data
- stolen credentials to access system
- snooping
  - IPC Order HO-013 (Rouge Valley Hospital, 2014)
    - staff selling new baby info RESP companies
  - interpersonal conflicts, personal gain, curiosity

Reducing Risk of Privacy Breaches

In determining what safeguards are applicable, consider:

- sensitivity and amount of information
- number and nature of people with access to the information
- threats and risks associated with the information

Reducing Risk of Privacy Breaches

1. Administrative
2. Technical
3. Physical

Reducing Risk of Privacy Breaches

1. Administrative

- privacy and security policies and procedures
- auditing compliance with rules
- privacy and security training
- data minimization ("need to know" limit)
- confidentiality agreements (alone or part of broader contracts)
- other means of communicating privacy messages (privacy notices, warning flags)
- privacy impact assessments

Reducing Risk of Privacy Breaches

2. Technical

- strong authentication and access controls
- detailed logging, auditing, monitoring (Rouge Valley)
- strong passwords, encryption (devices, documents, email)
- patch and change management
- firewalls, hardened servers, intrusion detection and prevention, anti-virus, anti-spam, anti-spyware
- protection against malicious and mobile code
- threat risk assessments, ethical hacks

Reducing Risk of Privacy Breaches

3. Physical

- controlled access to premises
- controlled access to locations within premises where identifying information is stored
- access cards and keys
- identification, screening, supervision of visitors

Privacy Breach Response

1. Implement, Identify, Contain

- implement privacy breach management policy
- determine if actual breach
- identify PI breached
- notify senior management
- containment measures to prevent further harm:
  - prevent further copies of records
  - ensure records retrieved/disposed of

Privacy Breach Response

2. Notify

- notice to individuals (*PHIPA* requires)
- form, timing of notice (direct or indirect?)
- notice should contain:
  - nature and extent of breach
  - nature and extent of PI
  - containment steps taken
  - any further actions the organization will take
  - be transparent!

Privacy Breach Response

2. Notify

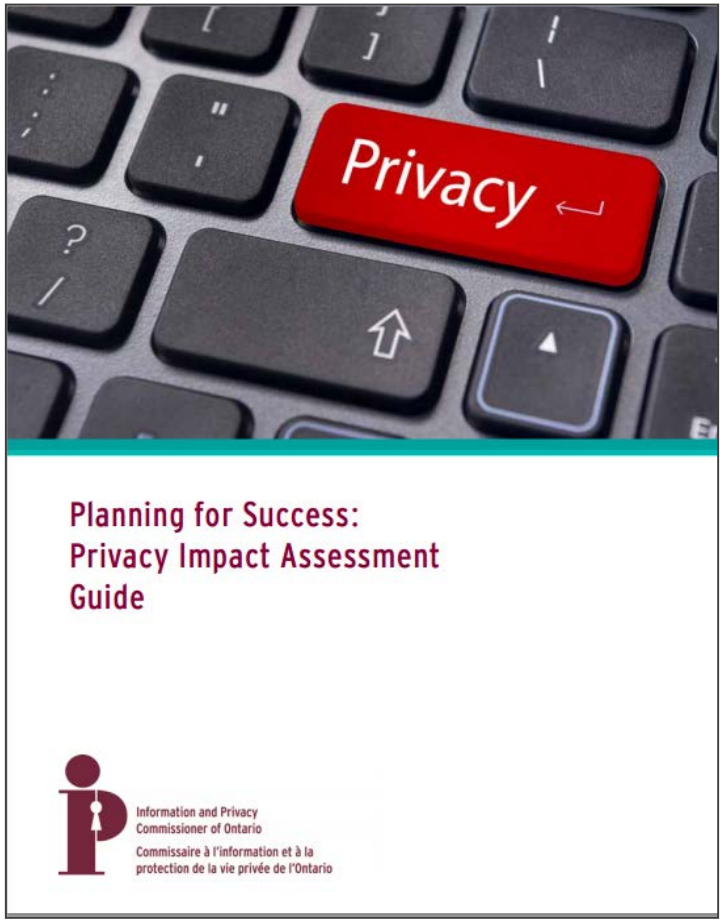
- notify oversight agency
- mandatory or advisable?

Privacy Breach Response

3. Investigate and remediate

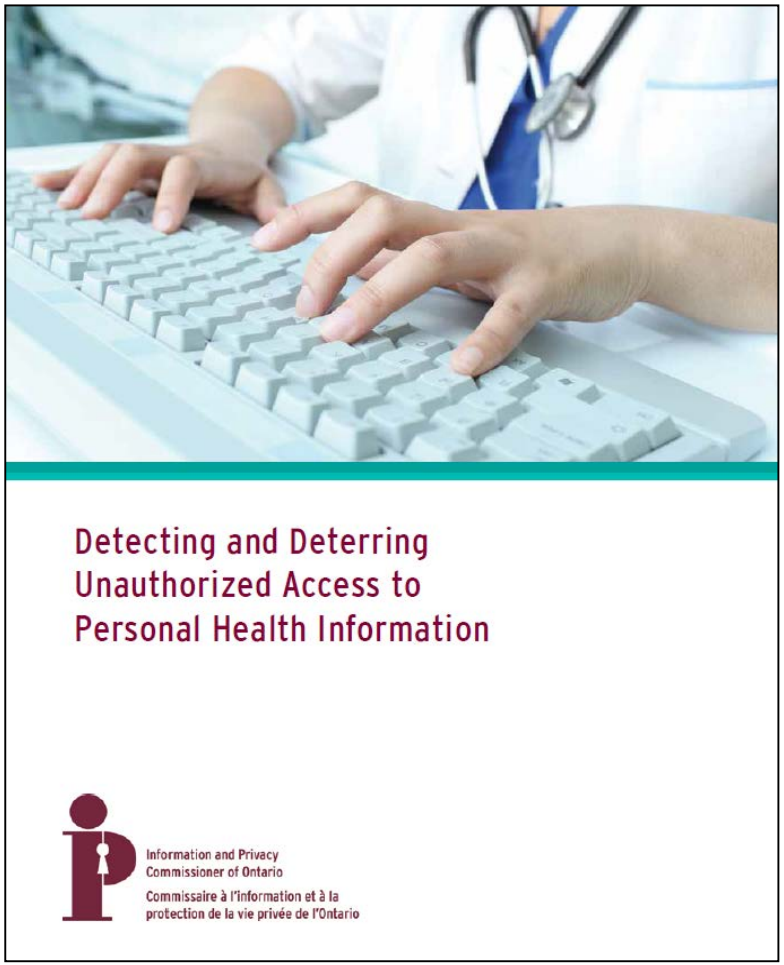
- conduct internal investigation to:
  - review containment measures taken
  - determine if breach effectively contained
  - ensure individuals notified
  - review circumstances of breach
  - review adequacy of policies and procedures
  - recommendations to prevent future breaches
- document investigation, recommendations
- implement recommendations

Planning for Success: Privacy Impact Assessment Guide



- tools to identify privacy impacts and risk mitigation strategies
- step-by-step advice on how to conduct a PIA

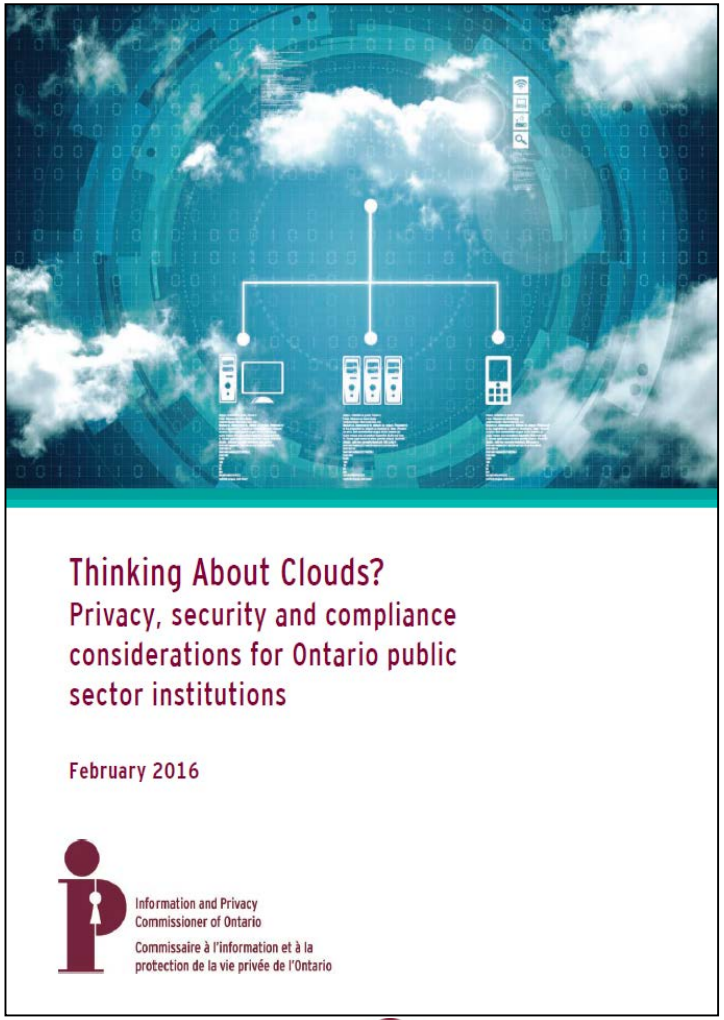
IPC Guidance on Snooping



- benefits and risks of electronic records
- impact of unauthorized access
- reducing the risk of unauthorized access
- recent ON convictions added deterrence

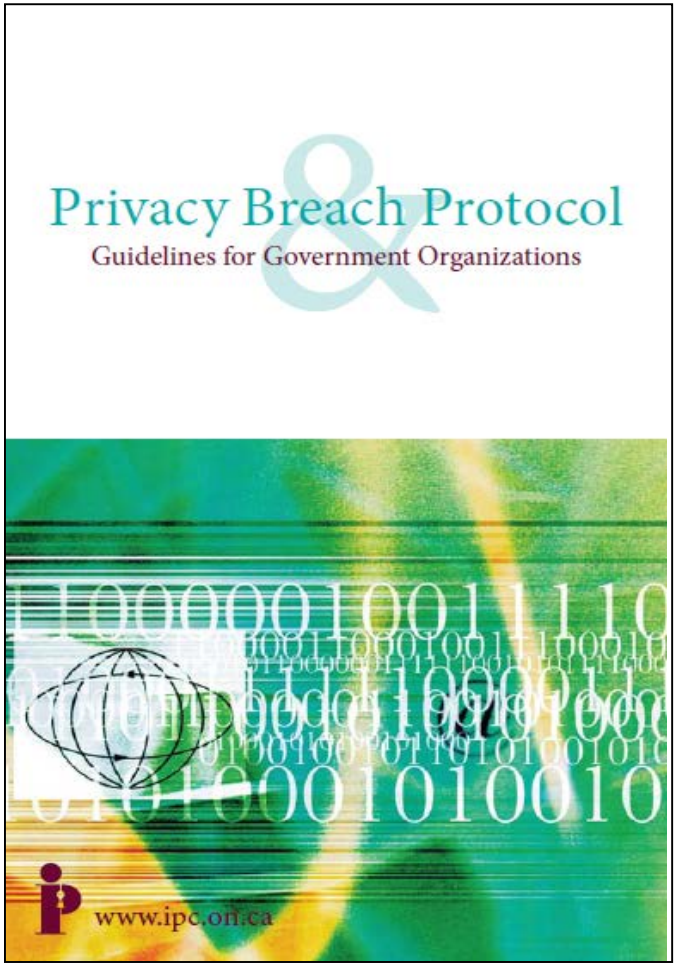
Thinking About Clouds?

- evaluate whether cloud computing services are suitable
- identify risks associated with using cloud computing
- outline strategies to mitigate risks
- aimed to assist smaller organizations



Privacy Breach Protocol

- privacy breach protocol helps identify privacy risks, potential and actual breaches
- ensure training on protocol
- ensure staff know their responsibilities when a breach occurs



Upcoming: Ransomware Guidance

- recent Ontario cases
  - two hospitals hit with attacks (Ottawa, Norfolk)
  - PHI did not appear to be breached in either case
- IPC will issue guidance
  - education about email attachments/links
  - critical to back up data, test backups
  - Up-to-date security software, anti-virus
  - automatic malware notices
  - [see Alberta IPC guidance]

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