Managing Privacy Breaches: Zone 5

Else Khoury

Seshat Information Consulting

Agenda

Part One:

- Legislative background
- Mandatory privacy breach reporting
- Privacy breach management as part of a privacy program
- What is a breach?

Part Two:

- Containment
- Evaluation of Risks
- Notification
- Prevention

Legislative Background

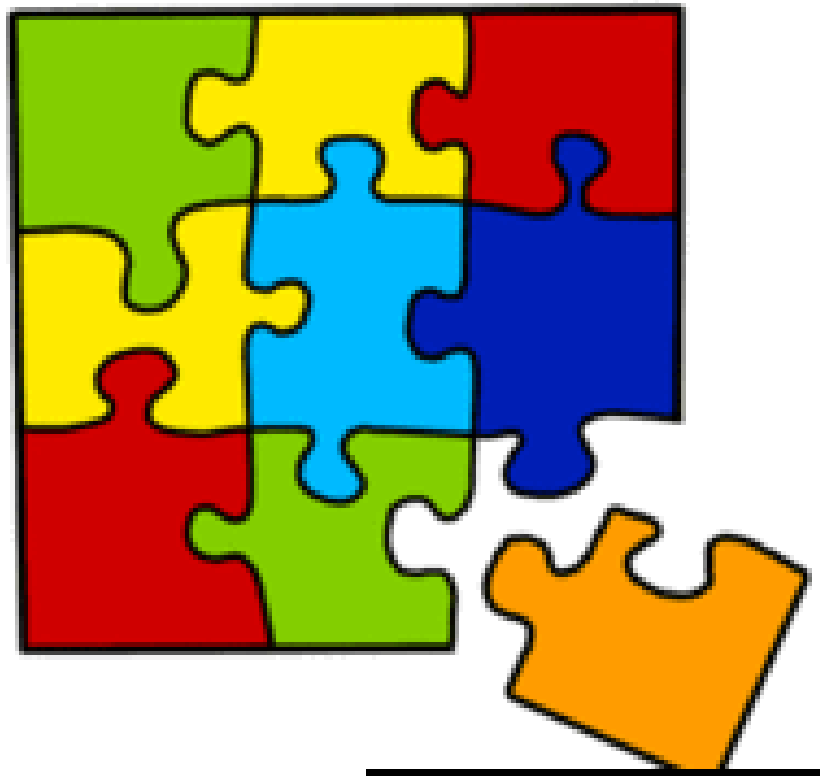
MFIPPA

- Balances right to access information with the obligation to protect privacy and right of individuals (not someone else) to access their own personal information (PI)

Personal Information (includes but is not limited to):

- Name, address, telephone number, email address, etc.
- Age, race, religion, sexual orientation, etc.
- Health information
- Financial information
- Employment/education history

Personally Information



Legislative Background

PHIPA

- Rules for the collection, use and disclosure of personal health information (PHI)
- Right of access to PHI
- Right to require correction or amendment
- Independent review of complaints

Mandatory Privacy Breach Reporting

- General Data Protection Regulation (GDPR) – May 2018
- Personal Information and Protection of Electronic Data Act (PIPEDA) – November 2018
- Personal Health Information Protection Act (PHIPA) – 2017
- Alberta, New Brunswick, Newfoundland and Labrador – Health Privacy Acts all contain mandatory reporting clauses

MFIPPA : Privacy Breach Reporting NOT Mandatory

But, probably not a bad idea

4,500 Ontario cannabis customers have personal data stolen

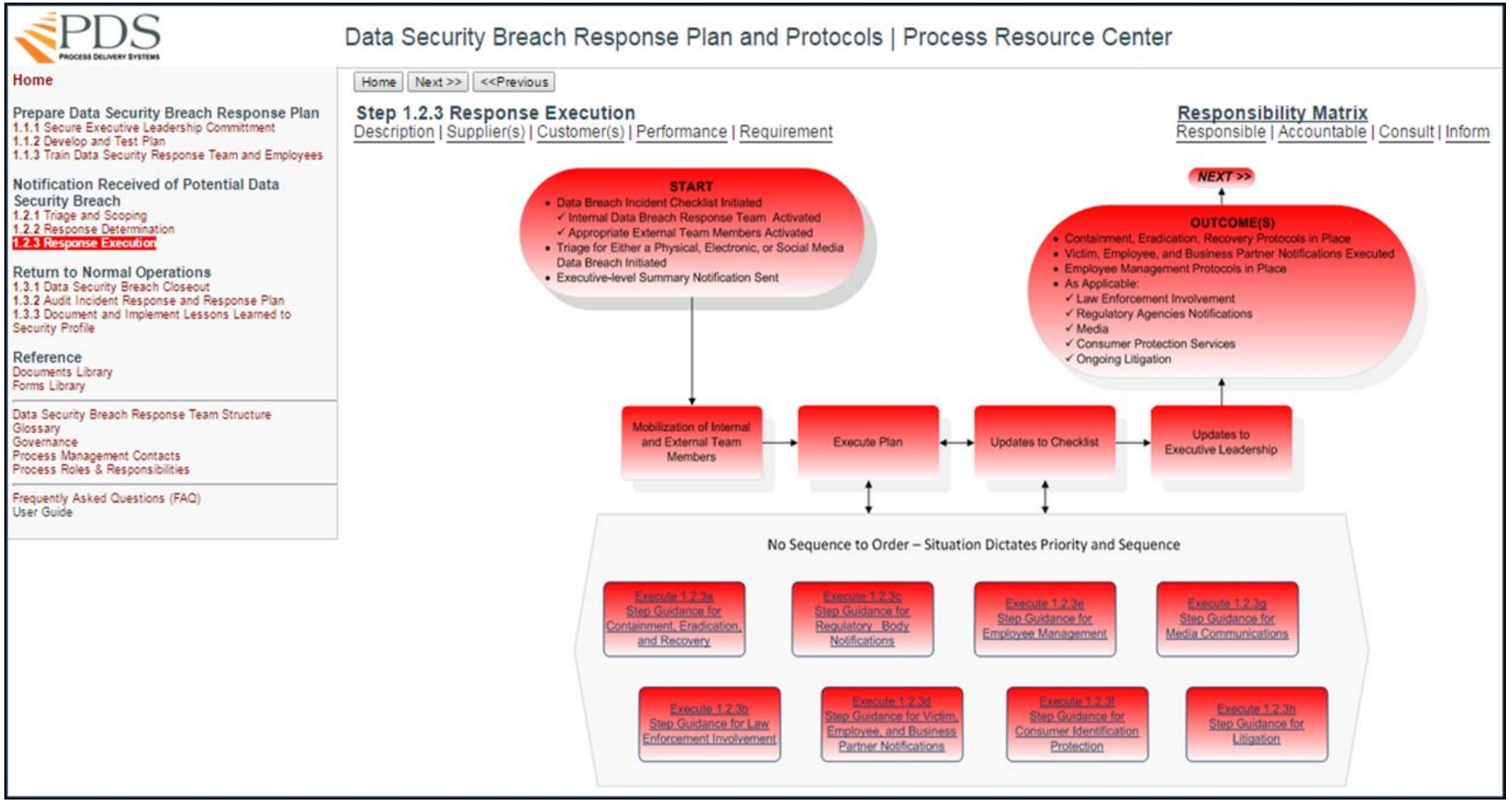
OCS says Canada Post to blame, but info obtained was limited

Muriel Draaisma · CBC News · Posted: Nov 07, 2018 12:57 PM ET | Last Updated: November 8, 2018

Privacy Breach Management as Part of a Broader Privacy Program

- In order to be successful at managing breaches, there should be a larger privacy program supporting your breach process, including:
  - Policy
  - Training
  - Senior management support
  - Governance
  - Accountability (Roles & Responsibilities)
  - Visibility
  - Third parties
  - Privacy Impact Assessments (PIAs)

Privacy Breach Response Plan



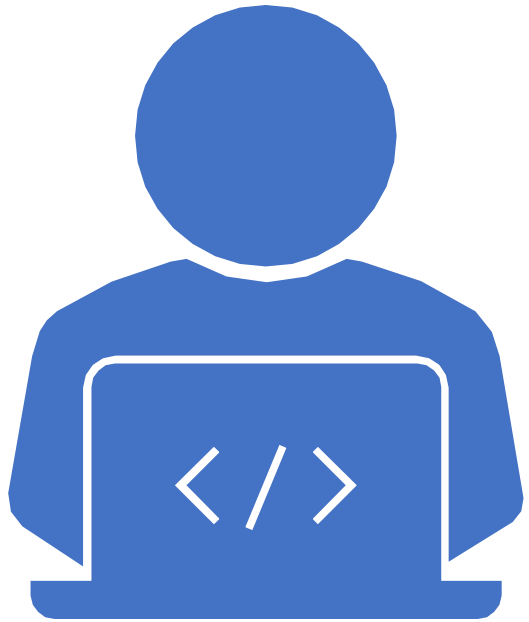
What is a Privacy Breach?

Information Privacy Commissioner of Ontario (IPC):

- Personal information is collected, retained, used, or disclosed in ways that are not in accordance with the provision of the Acts.

e.g. Personal Information that is lost (misplaced file), stolen (laptop) or hacked or inadvertently disclosed through human error (letter is mailed to the wrong address)

Source: IPC's "Privacy Breach Protocol, Guidelines for Government Organizations"



What is a Privacy Breach

Federal Privacy Commissioner:

- Improper or unauthorized creation, collection, use, disclosure retention, or disposal of personal information
- Material Privacy Breach: a breach that involved sensitive personal information and could reasonably be expected to cause injury or harm to the individual and/or involves a large number of affected individuals

Source: OPC's "Privacy Breach Management Toolkit"

There Are Breaches…

Durham Region Health class action lawsuit puts price on personal information

…and then there are breaches

Ashley Madison: 'Suicides' over website hack

By Chris Baraniuk
Technology reporter

24 August 2015

Share

Municipalities Targeted

Guidelines for Identifying a Breach

Some simple guidelines:

- Collection:
  - Do you need the information to provide the service?
  - e.g. registering a child in a swimming program:
    - Name
    - Age
    - Swimming level
    - Allergies
    - Parent/guardian
    - Name of cousin twice removed

Guidelines for Identifying a Breach

Use:

- Do you need the information/does someone else need the information in order to do your job/provide the service?
- e.g. When registering the child for swimming lessons, I do not need to know that my next door neighbour is his cousin twice removed

Guidelines for Identifying a Privacy Breach

Disclosure:

- Is it necessary to disclose the information I have collected/used in order to provide the service?
  - e.g. In the case of swimming lessons, the information collected (that is valid) needs to be shared with the coach who is coaching that child and the program manager, supervisor, etc.
  - The information does NOT need to be shared with another coach, the janitor, etc. UNLESS there is a specific reason to do so

Guidelines for Identifying a Privacy Breach

Retention:

- How long do you need to keep the information in order to provide the service?
    - Refer to your retention schedule AND FOLLOW IT!

Destruction:

- Destroy the information according to the records retention schedule
- ACTUALLY destroy it: paper, electronic, WHATEVER

Implementing a Privacy Breach Response Plan

What You Need:

- Senior level support
- Resources (training, policies, PR)
- Outcomes
  - Most privacy breaches are unintentional and should not be punished
  - Think about how your organization will respond to privacy breaches that are intentional (spoiler alert: involve IT)

Expect
Freaking Out

Be Kind

Before Containment

Federal Privacy Commissioner:

- Improper or unauthorized creation, collection, use, disclosure retention, or disposal of personal information
- Material Privacy Breach: a breach that involved sensitive personal information and could reasonably be expected to cause injury or harm to the individual and/or involves a large number of affected individuals

Source: OPC's "Privacy Breach Management Toolkit"

Before Containment: Recognizing a Breach

Names, banking information accidentally shared in emails to University of Waterloo students

'We sincerely regret the mistake and have apologized to the people impacted,' university says

CBC News · Posted: Mar 08, 2019 12:42 PM ET | Last Updated: March 8

Containment and Preliminary Assessment

1. Once the breach has been reported, ask:
   - Was it actually a breach
   - Who was affected
   - What information was compromised
   - How did the breach occur
   - Who received the information
   - What/who caused the breach
   - How can the information be contained/prevented from further breach

Containment and Preliminary Assessment

2. Put a team together to manage the breach. Include:
    - Privacy lead
    - Department/program lead

3. Begin a breach response:
    - In the case of a lost or stolen device, attempt to wipe the device remotely if possible
    - In the case of accidentally sending private information to the wrong person(s), try to retrieve the information
    - In the case of phishing/hack, contact law enforcement or implement a cyber-response

Containment and Preliminary Investigation

- Remove access to system or application in question
- Shut down the system or application in question
- Work with IT when the breach has been electronic
- Communicated with staff as you go (need to know basis) to ensure that the same mistake is not repeated

Third Party Breach?

- Contracts with third parties who have access to personal information or personal health information of our clients/residents/patients should contain provisions for a privacy breach response that is consistent with your municipalities (or better, since privacy breach reporting is now mandatory under PIPEDA)
- If you don’t have an expectation for adequate privacy breach response in your contract, you are at the mercy of the third party, leaving you open to litigation, etc.

You Can’t Outsource Accountability!

Documentation

Document all stages of the breach response

Develop a form which will document all stages of the breach response:

- How it occurred
- Who was involved
- Who managed the breach
- Whose information was involved
- How containment occurred
- How notification occurred
- Names, contact information, positions, etc.

Preliminary Assessment

- Consider developing a form that the privacy lead may use during the preliminary assessment in order to capture all relevant information

Evaluation of Risks: PI or PHI

1. What information was breached?
   - E.g. name, contact information, health information, financial information, etc.
2. How sensitive is the information breached?
3. What is the context of the breach?
   - E.g. mailing list of HIV patients vs. recreation participants
4. Was the information encrypted or otherwise protected?
5. How could the information be used?

Evaluation of Risks: Cause and Extent

- How did it happen?
- Is there a risk of further exposure?
- How big was the breach (to how many persons was the information released)?
- Was it lost or stolen?
- Has it been recovered? Can it be recovered?
- What has been done to mitigate?
- Is this a systemic problem or isolated incident?

Evaluation of Risk: Who is Affected?

How many people are affected?

Who are they?

- Employees
- Contractors
- Clients
- Other governments,
- Etc.

Source of the Breach

Was it an internal error or did it come from an external threat?

Accidental or intentional?

On premises or off?

What is the Harm?

Accidental mailing vs. hack

Who is the recipient (do they have a connection with the individual(s) affected)?

What harm could occur?

- Identity theft
- Financial loss
- Physical harm
- Reputation damage
- Legal penalties

What is the Harm?

1. What is the harm to the institution?
   - Loss of trust
   - Legal proceedings
   - Financial loss
   - Public health or safety

Notification

1. Notify internally:
   - Program manager, director, commissioner, etc.
   - Privacy program
2. Notify affected individuals:
   - What are your obligations to notify (operational/policy if not mandatory)
   - What is the level of harm
   - Consider calling AND sending a letter
3. Notify as soon as possible
4. Explain your PBRP
5. Explain their option to complain to the IPC

Notification: What to Include

- Description of the incident
- Source of the breach
- List of information breached
- Description of investigation
- Advice if required
- Contact information for privacy lead
- IPC contact information

Prevention/Mitigation

- Training and education
- Coaching/mentoring
- Policy
- Public relations/ad campaign
- Discipline
- Revocation of privileges

Prevention/Mitigation

- Revise/develop internal protocols
- Additional training for employees
- Tightening access/permissions
- Tightening auditing
- Encryption
- Third party contract language
- Security

MFIPPA : Privacy Breach Reporting NOT Mandatory

Lessons Learned

Use the opportunity post-breach to evaluate how well you responded as a team, and adjust accordingly

A well-managed breach can get your privacy program some currency in the organization (you saved us a $3 million lawsuit!)

Questions

else.khoury@outlook.com