

ENTER PASSWORD:

What we
Hear, Read, Say and **Do** *matter*

Information Privacy and Security

is *everyone's* responsibility

INCIDENT RESPONSE

Mike Tolfree
Manager, Information & Privacy
Calgary Health Region



calgary health region

Introduction

- Responding to breaches of the privacy and security of sensitive information.
- Suggested process to respond to breaches.
- Discuss issues that merit special consideration
- Walk through a complex “real world” example.



Introduction

- My role.
 - Manager of Information & Privacy at the Calgary Health Region.
 - Duties include:
 - privacy training
 - requests to access information
 - risk assessments of new information systems or project
 - auditing
 - records management
 - responding to breaches.

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region

Introduction

- Most of a privacy officer's responsibilities revolve around breaches.
 - react to reported security breaches.
 - proactive efforts to prevent breaches. (e.g. training, risk assessments, audit.)
- Both proactive and reactive responses to breaches are important.
- This presentation addresses how to react to a breach.



Introduction

- Calgary Health Region
 - One of the largest health regions in Canada, serving over 1 million individuals.
 - About 24,000 employees
 - 3 large acute care hospitals, 1 children's hospital, several smaller rural hospitals.
 - Many outpatient clinics
 - Countless community and other programs
- A robust EHR environment – many electronic applications.
- Ripe environment for breaches.

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region

Introduction

- Definition – What is a breach?
 - Any collection, use or disclosure of identifiable information that is not permitted by applicable privacy legislation or organization policy or procedures.
 - Breaches can range from misdirected mail or faxes, to inappropriate use of information systems, to stolen or lost computers.



Incident Response - Process

- Benefits of having an established process to respond to breaches.
 - React quicker in a crisis.
 - Improves moral authority during an investigation.



Incident Response - Process

- A breach is reported. What do you do?
 - Assess severity.
 - Obtain concise summary of the incident.

Concise Summary

- Who are the involved individuals? Victim, “perpetrator”, responsible manager.
- What happened?
 - Medium of breach? (Electronic, Paper)
 - Exactly what information was breached?
- Where did the breach occur? (facility, in the community, etc.)
- When did the breach happen? (How many days ago)
- Assess for severity.

Immediate Response

- Take steps (if possible) to immediately stop the breach.
 - Try to recover information that is the subject of the breach.
 - Send courier to pick up paper data (if applicable).
 - Consider shutting down software if that is the source of the breach.

Communication (Internal)

- Who in your organization needs to be notified of the breach?
 - Communications department?
 - Senior management?
 - IT (for technical issues?)
 - Health Records?
 - Human Resources?



Investigation

- Begin investigation after addressing the immediate danger/risk.
- More severe breaches need to be investigated more promptly.
- Interview the individuals involved with the breach.
- Work with the manager.
- May involve Human Resources if the breach involves employee misconduct.

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region

Investigation (con't)

- Determine exactly what happened, who was affected, responsible parties, etc.
- Determine the root cause of the breach.
- What actions will help prevent future breaches of this nature?



Notifying victims

- Do you notify affected individual(s)?
- Applicable law.
 - No mandatory reporting laws in most Canadian jurisdictions (except Ontario)
 - Rumors that mandatory reporting laws are coming.
 - Many states in the US require mandatory disclosure to any individual affected by security breach.
- Appear to be moving towards an industry standard to notify.



Notifying victims (con't)

- Individuals are usually more forgiving if they receive notice
- Conversely, be concerned about perceived “cover-ups”.
- Moral obligation? Individuals can be more alert to unusual activity.
- Will notification do more harm than good?
- I favor notification unless clear probability that it will result in additional harm.



Notifying victims (con't)

- Some of the factors to consider are:
 - Who has unauthorized possession of the information?
 - What is the potential for criminal activity?
 - Will notification cause significant additional harm?
 - What is the effect of media coverage surrounding the incident?
- Refer to matrix in materials



Content of Notice

- How to notify? (letter, phone or in-person meeting.)
 - Phone or meeting can be useful if someone in your organization has an ongoing relationship with the individual.
 - Less threatening when people hear it from a trusted source.
 - Make sure to document notice provided by phone or meeting.



Content of Notice (con't)

- Notification should
 - introduce who you are.
 - briefly describe the incident
 - state the steps you have taken to correct the issue.
 - reference other resources for additional education
 - Contain contact information of your office if any questions.
 - Apologize for the incident.
 - Provide contact information for the Privacy Commissioner.
- Normal mail vs. registered mail.



Self-Reporting a Breach

- Similar analysis as above.
- At a minimum, report significant breaches with potential to cause harm.
- Report any breach that could generate publicity.
- Report if you notify the victim.
- Internal vs. external breach.

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region

Self-Reporting a Breach (con't)

- Proactive reporting to media? (only for very serious breaches.)
- Commissioner may open a separate investigation, but not always.
- Self-reporting is often a mitigating factor.



Form of Breach Report

- Document findings of the investigation in a formal report.
- The report is a record of the incident, and your organization's response.
- Can be useful as a reference for external investigation.
- Can be useful in employee grievance or arbitration.
- Be careful of report "tone".
- The report should be a concise and professional document.



Report content

- What is the source of the breach?
- Describe information breached.
- Who did you interview?
- What actions did you take?
- Where did the breakdown occur?
- Recommendations to mitigate/prevent.
 - Correct the source of the breach.
 - Could include employee discipline.
- See template reporting form.

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region

Employee Discipline

- Discipline may be appropriate for some breaches.
- Promote accountability/change culture.
- Work closely with Human Resources.
- Union rules/CBAs often play a significant role.
- Factors to consider.
 - Intentional?
 - Active misconduct or malice?
 - Repeat offender?

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region

Internal Tracking

- Keep statistics on breaches.
 - type of breach (make several broad categories),
 - individual and unit/department that is the source of the breach,
 - date of the breach.
- Common breaches
 - Misdirected fax/mail
 - Lost charts/documents.
 - Wrong health information disclosed.
 - Theft
 - Inappropriate employee access (snooping)
 - Unauthorized disclosures of information (e.g. without consent or in contravention of legislation.)

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region

Internal Tracking

- Periodically review statistics, compile into user friendly graphs/charts.
- Look for trends:
 - High number from one user?
 - High number from one department?
 - Unusually low numbers?
 - Common types of breaches?
- Compare against prior years.
- Statistics help focus training and education efforts.

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region

Real World Scenario

- In the fall of 2006, a Region laptop was stolen from an employee's house.
- Examine how the Region's breach process worked in this situation.



Real World Scenario

- Privacy Office notified the day after the theft.
- Assessed severity of incident.
 - Laptop contained database with information about mental health patients.
 - Information was sensitive.
 - Harm could definitely result from misuse of data.



Stop immediate harm

- Laptop is already gone, unable to recover it.
- File police report.
- Lock-down other laptops in the program.
- Other staff members of this program are not allowed to take laptops outside of CHR Facilities.



Communicate

- Internal Stakeholders:
 - Mental Health
 - IT Security
 - Communications
 - Legal
 - Quality and Safety of Health Information
(for expertise in handling Critical Incidents)



Communicate

- External Stakeholders
 - Privacy Commissioner
 - Alberta Health & Wellness
 - Child Youth & Family Services (many joint patients.)
- Daily meetings.



Investigation

- Interviewed employee, manager, technical resource.
- Protections in place
 - 3 layers of passwords
 - Password memory not activated.
 - Employee had received privacy training.
- Potential weaknesses
 - A locking cable not used
 - Data was not encrypted.
 - Entire database was loaded on the laptop
 - Possibly weak passwords.

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region

Notification

- Privacy Commissioner promptly notified.
- Notify the affected patients?
 - Mental Health concerns.
 - Low risk of actual harm,
 - Notification could do more harm than good.
 - Decided to notify. [Refer to matrix]
 - Letter sent by registered mail.
- Proactively inform the media
 - Media informed after we start notifying patients.
 - Want affected patients to hear from the Region first.

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region

Notification

- Notify patients of incident and risks of identity theft.
- Advise the patient to be alert for unusual activity.
- Provide resources to help patient
 - information about credit reports
 - help monitor credit rating.
 - offer to help.
- Set up help phone line.
- Set up process so that patients can view their information that was in the database.

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region

Report

- Breach caused by several factors.
 - Failure to follow appropriate security policies.
 - Failure to encrypt.
 - Failure to secure laptop
 - Storing more patient data than necessary on the laptop.
 - Insufficient security training and oversight.



Report

- All patient data on laptops or other mobile devices must be encrypted.
- Only store the minimum data necessary on laptops.
- Utilize wireless connections when possible.
- Conduct Security/Privacy reviews of facilities.
- All removable media (USB drives, CDs, etc.) must be encrypted.



Employee Discipline

- Employee had not followed all policy requirements.
- Employee believed the data was secure (because of password protection.)
- Stored laptop in a place believed to be secure (house)
- No previous security violations/incidents.
- Certainly no intent to have laptop stolen.
- Discipline not appropriate - Retrain.



Conclusion

- Having an established process is important.
- Enables you to respond quickly and thoroughly to security incidents.
- Scalable to address small to large breaches.
- Increases confidence in your area.



What we
Hear, Read, Say and **Do** *matter*
Information Privacy and **Security**
is **everyone's** responsibility



QUESTIONS?

iweb.calgaryhealthregion.ca/infoprivacy/index.htm



calgary health region