Privacy Breach Management

ATTENTION: All practice managers, healthcare providers, clinic managers of private healthcare practices. This Document Management Tip has been created especially for you.

60% of small and medium business owners go out of business

within 6 months after a **privacy and security breach**. Properly managing a privacy breach is a critical to the continued success of your business. After you identify a breach you must contain the breach, prevent it from happening again, and rebuild trust with your patients and clients.

This Document Management Tip will help you:

- Document the incident
- Prepare a report to regulators and stakeholders
- Prevent it from happening again
- Improve training to your team
- Identify safeguards to better protect personally identifying information and health information

What to do next:

- Instantly download this free Documents Management Tip – Privacy Breach Management
- Discuss with your team and revise to best meet the needs of your practice

Need more?

- Register for on-line Privacy, Confidentiality, and Security webinar series
- Document Management Tips for your practice Management

BONUS Instant access to Privacy Breach Awareness video, "Can you spot a privacy breach? (What are you going to do about it?)"

BONUS Share this infographic with tips that you can share with your team.

Using this Document Management Tip gives you:

- A tool that you can use right away to improve your privacy breach management practices
- Employee training that is cost effective and convenient
- Tips to improve privacy and security
- Tips to manage your business risks

It is expected that you will review and refine these documents to meet your needs.

This publication provides general guidance for healthcare practices in Alberta. For additional assistance, please contact Information Managers Ltd.

Jean L. Eaton
Practical Privacy Coach and Practice Management Mentor

author of the forthcoming books, "*Privacy Breach Management Resource Package*" and *"Practice Management: Easy to Follow Steps to Start a New Clinic and Improve Your Established Clinic".*

Please join one or more of our LinkedIn Groups:

Practical Privacy in Healthcare

Practice Management Nuggets

October 2014

Document Management Tip

Privacy Breach Management

Background

A privacy breach can take place when there is unauthorized access to or collection, use, disclosure or disposal of personally individually identifying or health information.

Reporting a privacy breach

Reporting a privacy breach is not currently mandatory under the *Health Information Act* (HIA)[1] or the *Freedom of Information and Protection of Privacy Act* (FOIP). However, **it is mandatory to report certain privacy breaches to the Commissioner under section 34.1(1) of Personal Information Protection Act.** PIPA organizations are required to notify the Commissioner of incidents "involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual."

Reporting a breach to the OIPC allows the OIPC to support your clinic in responding to the breach and ensures all in the program learn from the breach.

A (suspected) privacy breach should be identified and reported to the Clinic Manager and the Privacy Officer.

The Privacy Officer will respond immediately to the breach and take immediate common sense steps to limit the breach. These steps will include:

- Immediately contain the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached, revoking access or correcting weaknesses in physical security.
- Notify the police if the breach involves theft or criminal activity

[1] See our article, "Mandatory privacy breach reporting proposed for Health Information Act"

The Privacy Officer, with assistance of the attending physician will:

- Ensure any breach involving Netcare is reported to Netcare's Information Access and Privacy Office immediately.
- Evaluate the risks associated with the breach and will consider
    - personal or health information involved
    - cause and extent of the breach
    - individuals affected by the breach
    - foreseeable harm from the breach
- Initiate a Privacy Breach Report
- Consider notification to
    - affected individuals
    - legislation requirements
    - contractual obligations
    - risk of identity theft or fraud
    - risk of physical harm
    - risk of hurt, humiliation or damage to reputation
    - risk of loss of business or employment opportunities
- Consider whether the following authorities or organizations should also be informed:
    - police
    - insurers or others
    - professional or other regulatory bodies
    - credit card companies and/or credit reporting agencies
    - Office of the Information and Privacy Commissioner

Privacy Officer will review the Privacy Breach Report and

- Ensure that immediate steps to mitigate the risks associated with the breach have been undertaken
- Consider notification of regulators to police, individuals
- Recommend appropriate communication plan to persons involved, staff, public, etc
    - Make decisions on notification
    - Communicate internally and externally
- Investigate the cause of the breach and preventative action taken. This may include
    - Security audit
    - Threat risk analysis to affected individuals
    - Policies and procedures reviewed and updated to reflect the lessons learned
    - Plan for an audit at the end of the process to ensure that the prevention plan has been fully implemented
- Staff education, sanctions
- Ensure front'-line staff are prepared to answer questions

Personal Information Protection Act (PIPA)

Organizations regulated by PIPA are REQUIRED to notify the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of personal information, where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the incident (PIPA section 34.1). A Report to the Commissioner must comply with section 19 of the *PIPA Regulation* and, among other things, must include "an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure." Considering the factors set out above may assist PIPA organizations in assessing the real risk of harm to individuals that could result from a breach incident.

Amendments to PIPA in May 2010 added new powers authorizing the Commissioner to require organizations to notify individuals affected by a reportable breach.

Notification to Individuals

Notification should include the following information:

- Date on which or time period during which the breach occurred*;
- Description of the circumstances of the breach (a general description of what happened)*;
- Description of the information involved in the breach* (e.g. name, credit card numbers, SINs, medical records, financial information, etc.);
- Identify risks so individuals can make their own decisions on how to protect themselves
- Description of any steps taken to reduce the risk of harm*;
- Next steps planned and any long term plans to prevent future breaches;
- Steps the individual can take to further mitigate the risk of harm. Provide information about how individuals can protect themselves e.g. how to contact credit reporting agencies (to set up a credit watch), how to change a personal health number or driver's license number.
- Contact information of a person who can answer questions about the breach*;
- Inform the individual that you have informed the OIPC and other relevant authorities such as police, professional regulators, etc
- Individuals have a right to complain to the Office of the Information and Privacy Commissioner. Provide contact information.

References and Resources:

To notify the OIPC about a privacy breach under PIPA, use the reporting form from:
Office of the Information and Privacy Commissioner, Alberta. "Reporting a Privacy Breach to the Office of the Information and Privacy Commissioner of Alberta"

Privacy Breach Reporting Form

Report Date:

Contact Person:
Name:
Title:
Phone:
Fax:
Email:
Mailing Address:

Risk Evaluation:

Describe the nature of the breach and its cause:

Date of incident:

Date incident was discovered:

Describe how the incident was discovered:

Location of incident:

Estimated number of individuals affected:

Type of individuals affected:
Client / customer / patient Employee Other

Personal Information Involved:
(Describe the personal or health information involved in the breach (e.g. name, address, health care number, financial, medical information), the form it was in (e.g. paper records, electronic database). Note: do not send identifiable personal information to the Office of the Information and Privacy Commissioner (OIPC).

Safeguards

Describe the types of physical security devices employed at the time of the incident (locks, alarm systems, etc).

Describe your technical security precautions (encryption, passwords, etc.).

Identify the type(s) of harm that may result from the breach:

- Risk of identify theft (most likely when the breach includes the loss of health insurance numbers, credit card numbers, debit card numbers with password information and any other information that can be used to commit financial fraud)
- Risk of physical harm (when the loss of information places any individual at risk of physical harm, like stalking or harassment)
- Hurt, humiliation, damage to reputation (associated with the loss of information such as mental health records, medical records, or disciplinary records)
- Loss of business or employment opportunities (usually as result of damage to the reputation of an individual)
- Breach of contractual obligations (contractual provisions may require notification of third parties in the case of data loss or a privacy breach)
- Future breaches due to similar technical failures (notification to the manufacturer may be necessary if a recall is warranted, and/or to prevent a future breach by other users)
- Failure to meet professional or certification standards (notification may be required to a professional regulatory body or certification authority)
- Other (please specify)

Notification

Has your privacy officer or responsible affiliate been notified?

- Yes Who was notified and when?
- No When will they be notified?

Have the police or other authorities been notified (professional authorities or the person required under contract)?

- Yes Who was notified and when?
- No When will they be notified?

Have affected individuals been notified?

- Yes Form of notification and when?
- No When will they be notified?

Describe the notification process (who was notified, the form and content of notification. Please provide a copy of the notification to the OIPC).

You may wish to provide the OIPC with any additional information you have collected regarding the breach, including:

- Steps that have been taken to reduce the risk of harm (like the recovery of information, locks changed, computer systems shut down),
- Internal investigation reports or findings
- Long term strategies you intend to implement to correct the situation (staff training, policy development, etc.)

Education

What additional educational pieces have been developed to prevent future breaches?

How can you educate and inform:

- Individuals directly involved in the privacy breach
- Your organization

Have you:

- Updated your privacy policies and procedures
- Provided your staff with adequate training
- Provided your staff with privacy policies and procedures for review

What sanctions (if any) have been applied to individuals directly involved in the privacy breach?

Reporting

If you intend to seek advice from the OIPC regarding how to respond to the breach and what actions should be taken, you should **report the incident as soon as possible** even where the above information is not yet available.

Once completed, submit the Privacy Breach Report form to the OIPC at the address below. It is preferable to submit the form by fax when timing is an issue.

Office of the Information and Privacy Commissioner
Calgary (PIPA): #500, 640 - 5 Avenue SW
Calgary, Alberta T2P 3G4
Fax: (403) 297-2711
Phone: (403) 297-2728

Edmonton (FOIP and HIA): #410, 9925 - 109 Street
Edmonton, Alberta T5K 2J8
Fax: (780) 422-5682
Phone: (780) 422-6860
Toll Free: 1-888-878-4044
Email: generalinfo@oipc.ab.ca

Organizations regulated by PIPA are **required** to notify the Commissioner of any incident involving the loss of, unauthorized access to, or disclosure of personal information, where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the incident (PIPA section 34.1)

To notify the OIPC about a privacy breach under PIPA, use the reporting form "Reporting a Privacy Breach to the Office of the Information and Privacy Commissioner of Alberta"

This publication provides general guidance for a Medical Office. Consultation with your Information Systems, Health Records, and Privacy Office is recommended. For additional assistance, contact Information Managers.