



Privacy and notifiable data breach – what it means for you

Dr Peter Walker – GP, Risk Advisor

Annual Women's and Children's Health Update - HealthEd

2018

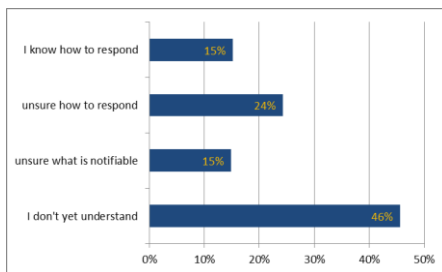
Agenda

- > Why do you need a "data breach response plan"?
- > What is a notifiable breach?
- > What do really you need to do?



2

Do you need a data breach response plan?



Source: Avant survey data 2017/18

Annual Women's and Children's Health Update - HealthEd February 2018

3

Healthcare data is vulnerable

Data of over 220,000 organ donors pledgers leaked online

Red Cross apologises after mass leak of Australian blood donor records

'Professional' hack on Norwegian health authority compromises data of three million patients

Dark family secrets: Anonymous letter uncovers child welfare records

Cosmetic surgery online mistake allows public viewing of women's photos, private details

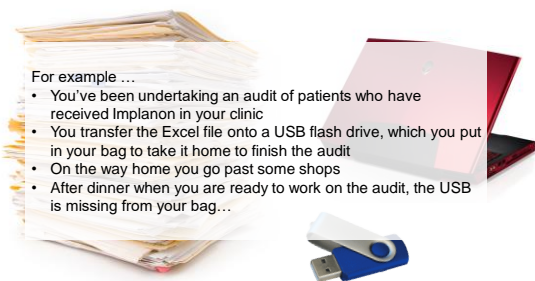
Hundreds left vulnerable to hackers after Johnson and Johnson data blunder

BREACH BENCHMARK REPORT: YEAR IN REVIEW
5.6M Patient Records Breached in 2017, as Healthcare Struggles to Comprehensively and Proactively Detect Health Data Breaches

Annual Women's and Children's Health Update - HealthEd February 2018

1

Could this be you?



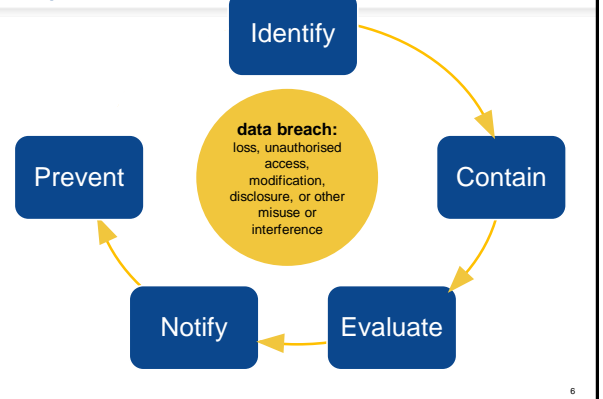
For example ...

- You've been undertaking an audit of patients who have received Implanon in your clinic
- You transfer the Excel file onto a USB flash drive, which you put in your bag to take it home to finish the audit
- On the way home you go past some shops
- After dinner when you are ready to work on the audit, the USB is missing from your bag...

Annual Women's and Children's Health Update - HealthEd February 2018

5

Response



Annual Women's and Children's Health Update - HealthEd February 2018

6

Avant mutual

Do you know or suspect there has been a data breach?

Yes

A data breach is:

- Unauthorised access to or unauthorised disclosure of personal information or
- Lost personal information and likely unauthorised access or disclosure

Likely to result in serious harm

Consider:

- Type of information and sensitivity
- Protections in place to prevent disclosure
- Persons who have obtained or could obtain data
- Nature of harm and number of people affected

Serious harm can be psychological, emotional, physical, reputational or financial.

Notification statement

Must include:

- Identity and contact details of practice
- Description of data breach
- Kind of information involved
- Recommendation about steps to take in response to breach

Is the breach likely to result in serious harm to an individual? (assess as soon as possible and within 30 days)

Yes

Can remedial action be taken to prevent the likelihood of serious harm?

Yes → No need to report

No → Notifiable data breach → Practice must notify individuals at risk of harm and OAC, as soon as practicable (via notification statement)

No → No need to report

Commenes 22 February 2018

7

Avant mutual

Notify

Who to notify?

How to notify?

What information to provide?

Notifiable Data Breach Form

Annual Women's and Children's Health Update - HealthEd February 2018

8

Avant mutual

Prevention is better than cure

9

Avant mutual

Back to the example

Identify

The loss of the USB is clearly a data breach

data breach: loss, unauthorised access, modification, disclosure, or other misuse or interference

Prevent

What can you prevent breach in future?

Contain

Is there anything you can do to contain the breach?

Evaluate

Is the breach likely to cause serious harm?

Notify

if you can't prevent serious harm

10

Avant mutual

What can I do now?

- Be aware of privacy and security obligations.
- Review information handling practices, procedures and systems.
- Review contracts with third party providers.
- Implement mitigation strategies.
- Know what to do if you discover a breach.

Annual Women's and Children's Health Update - HealthEd February 2018

11

Avant mutual

Where can I find more information?

- Office of the Australian Information Commissioner www.oaic.gov.au/
- Australian Digital Health Agency www.digitalhealth.gov.au/
- Australian Cybersecurity Centre www.acsc.gov.au/
- Australian Signals Directorate www.asd.gov.au/publications/protect/essential-eight-explained.htm
- Stay Smart online Information Security Guide for small healthcare businesses www.staysmartonline.gov.au/
- Avant www.avant.org.au

Annual Women's and Children's Health Update - HealthEd February 2018

12

Important notices

General disclaimer

The information in this presentation is general information relating to legal and/or clinical issues within Australia (unless otherwise stated). It is not intended to be legal advice and should not be considered as a substitute for obtaining personal legal or other professional advice or proper clinical decision-making having regard to the particular circumstances of the situation.

While we endeavour to ensure that documents are as current as possible at the time of preparation, we take no responsibility for matters arising from changed circumstances or information or material which may have become available subsequently. Avant Mutual Group Limited and its subsidiaries will not be liable for any loss or damage, however caused (including through negligence), that may be directly or indirectly suffered by you or anyone else in connection with the use of information provided in this presentation.

