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

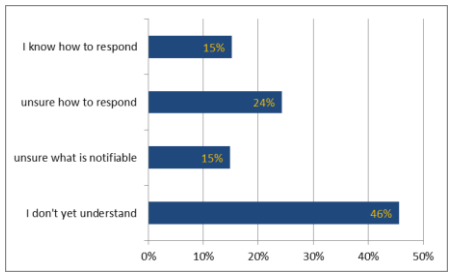
Agenda

> Why do you need a "data breach response plan"?

> What is a notifiable breach?

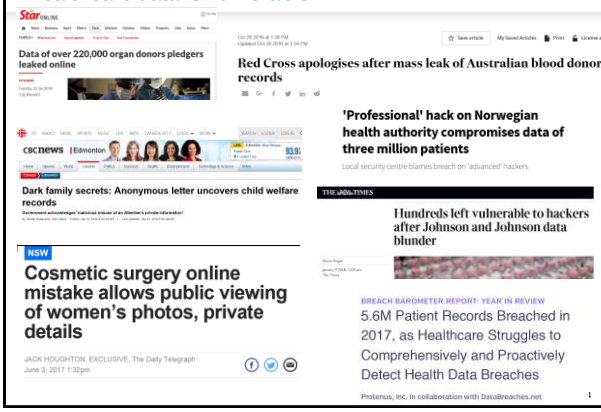
> What do really you need to do?

Do you need a data breach response plan?



Source: Avant survey data 2017/18

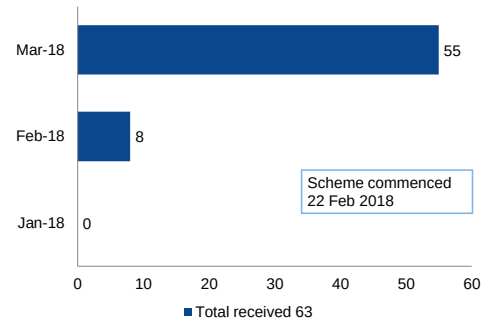
Healthcare data is vulnerable



Healthcare data is vulnerable

> Just ask Family Planning NSW!

Total notifications received by OAIC



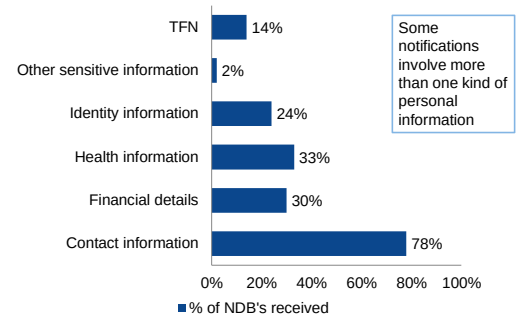
https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/Notifiable_Data_Breaches_Quarterly_Statistics_Report_January_2018__March_.pdf

Top 5 industry sectors

Top 5 industry sectors	NDB's received
Health service providers	15
Legal, Accounting and Management	10
Finance	8
Education	6
Charities	4

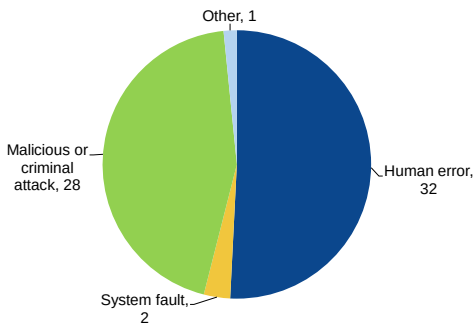
https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/Notifiable_Data_Breaches_Quarterly_Statistics_Report_January_2018__March_.pdf

Kinds of personal information



https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/Notifiable_Data_Breaches_Quarterly_Statistics_Report_January_2018__March_.pdf

Source of the breach



https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/Notifiable_Data_Breaches_Quarterly_Statistics_Report_January_2018__March_.pdf

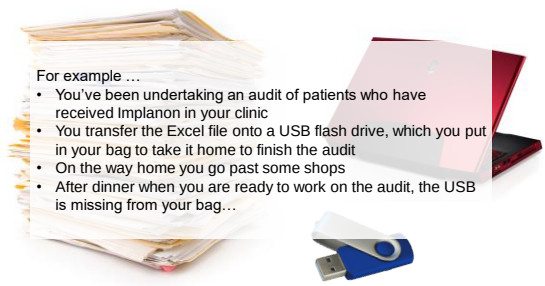
Number of people affected

Unknown	0
10,000,000 or more	0
1,000,000 – 9,999,999	0
100,000 – 999,999	0
10,000 – 99,999	3
1000 – 9999	3
100 – 999	11
10 – 99	9
2 – 9	17
1	20

https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/Notifiable_Data_Breaches_Quarterly_Statistics_Report_January_2018__March_.pdf

10

Could this be you?

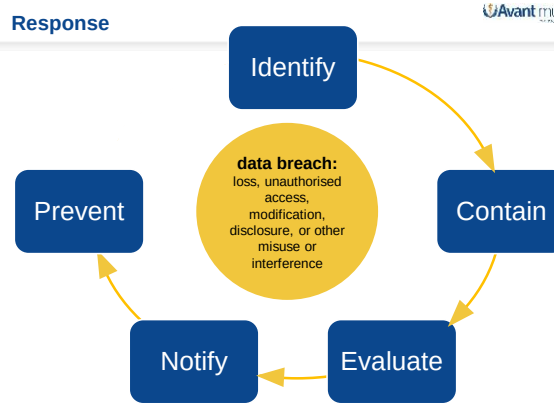


For example …

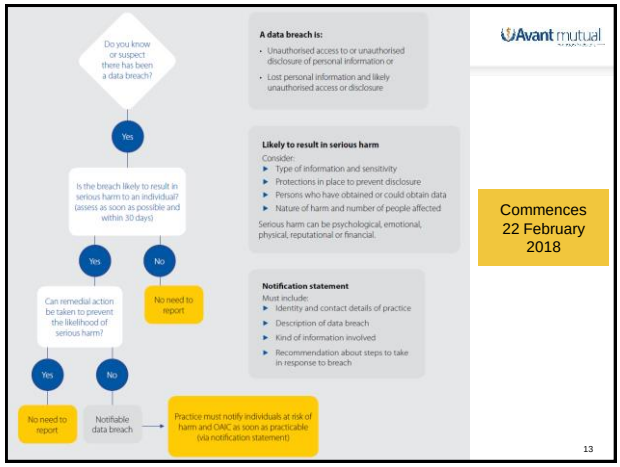
- You've been undertaking an audit of patients who have received Implanon in your clinic
- You transfer the Excel file onto a USB flash drive, which you put in your bag to take it home to finish the audit
- On the way home you go past some shops
- After dinner when you are ready to work on the audit,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

11

Response



12



Commences 22 February 2018

13

Notify

Who to notify?

How to notify?

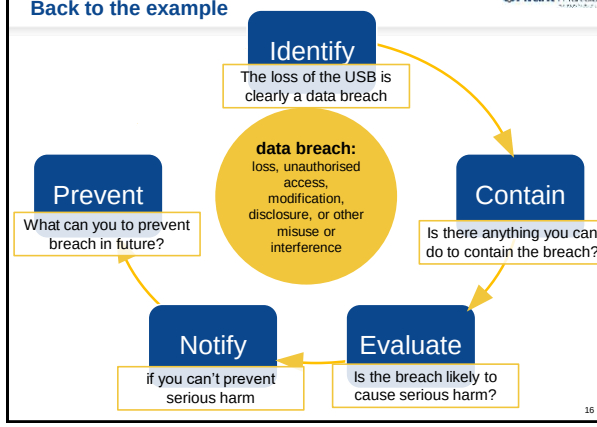
What information to provide?

14

Prevention is better than cure

15

Back to the example



16

What can I do now?

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

17

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

18

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.

Avant mutual
by doctors for doctors