



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

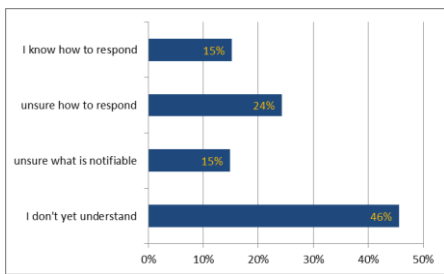
2018

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

Data of over 220,000 organ donors pledged 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

5.6M Patient Records Breached in 2017, as Healthcare Struggles to Comprehensively and Proactively Detect Health Data Breaches

Healthcare data is vulnerable

> Just ask Family Planning NSW!

Family Planning NSW targeted by hackers with ransom demand, data of 8,000 people at risk

Up to 8,000 clients could be affected by the hack, which occurred more than two weeks ago.

These databases contained information from around 8,000 clients who had contacted Family Planning NSW through our website in the past two and a half years, seeking appointments or leaving feedback, the email read.

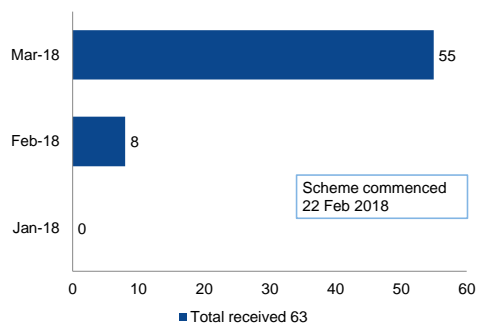
The email claimed the hackers demanded a \$15,000 bitcoin ransom on Anzac Day, and was sent on the following day.

Statement on Family Planning NSW

14 May 2018

The Office of the Australian Information Commissioner was notified by Family Planning NSW about a data breach incident that occurred on 25 April 2018. The Oaic understands that Family Planning NSW is in the process of notifying individuals whose personal information may have been affected by the breach.

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_ppdf

Top 5 industry sectors


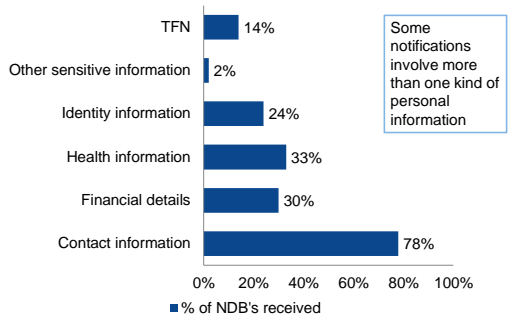


| Top 5 industry sectors | NDB's received |
|----------------------------------|----------------|
| Health service providers | 15 |
| Legal, Accounting and Management | 10 |
| Finance | 8 |
| Education | 6 |
| Charities | 4 |



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


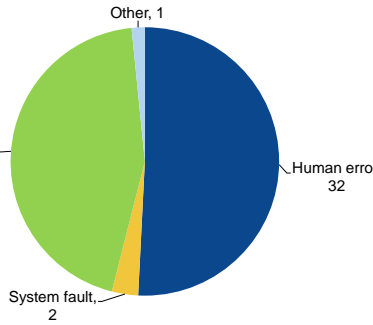



| Kind of personal information | % of NDB's received |
|------------------------------|---------------------|
| Contact information | 78% |
| Health information | 33% |
| Financial details | 30% |
| Identity information | 24% |
| TFN | 14% |
| Other sensitive information | 2% |

Some notifications involve more than one kind 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


| Source of the breach | Count |
|------------------------------|-------|
| Human error | 32 |
| Malicious or criminal attack | 28 |
| System fault | 2 |
| Other | 1 |

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


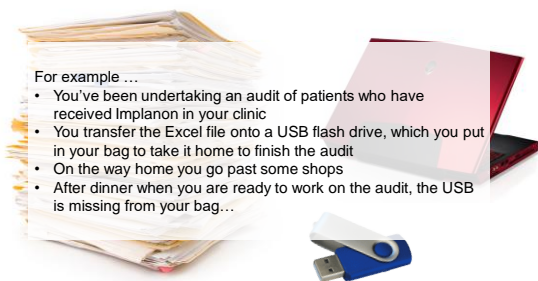


| | |
|-----------------------|----|
| Unknown | 0 |
| 10,000,000 or more | 0 |
| 1,000,000 – 9,999,999 | 0 |
| 100,000 – 999,999 | 0 |
| 10,000 – 99,999 | 3 |
| 1000 – 9999 | 3 |
| 100 – 999 | 11 |
| 10 – 99 | 9 |
| 2 – 9 | 17 |
| 1 | 20 |



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


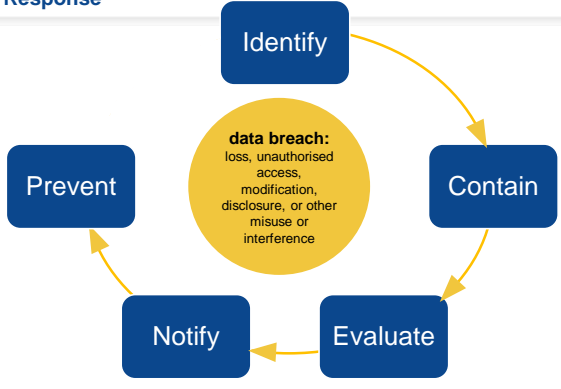
Could this be you?

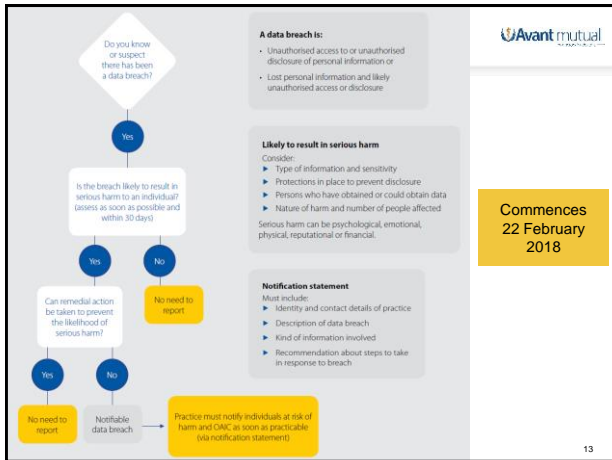
For example ...

- 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...

Response

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

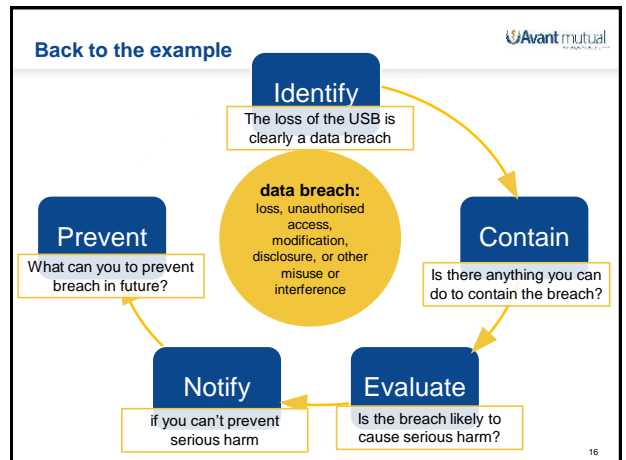


Notify

Who to notify?

How to notify?

What information to provide?



- ## 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.
-

- ## 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
-

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.