



Health data breaches: Negotiating complexity in Australia's new notification scheme

Dr. Megan Prictor

Research Fellow

Health, Law and Emerging Technologies programme

Melbourne Law School

Twitter: @MeganPrictor





Data breaches

- Unauthorised access or disclosure, or loss
- Focus is on ‘personal’ information
- Serious, harmful data breaches now almost ‘routine’
- Hacking and human error
- How to mitigate harm??



Security

Healthcare tops UK data breach chart – but it's not what you're thinking

WannaCrypt? Actually human error is the biggest problem

By John Leyden 1 Jun 2017 at 12:45

14 SHARE



The UK health sector accounts for nearly half (43 per cent) of all data breaches, according to new research.

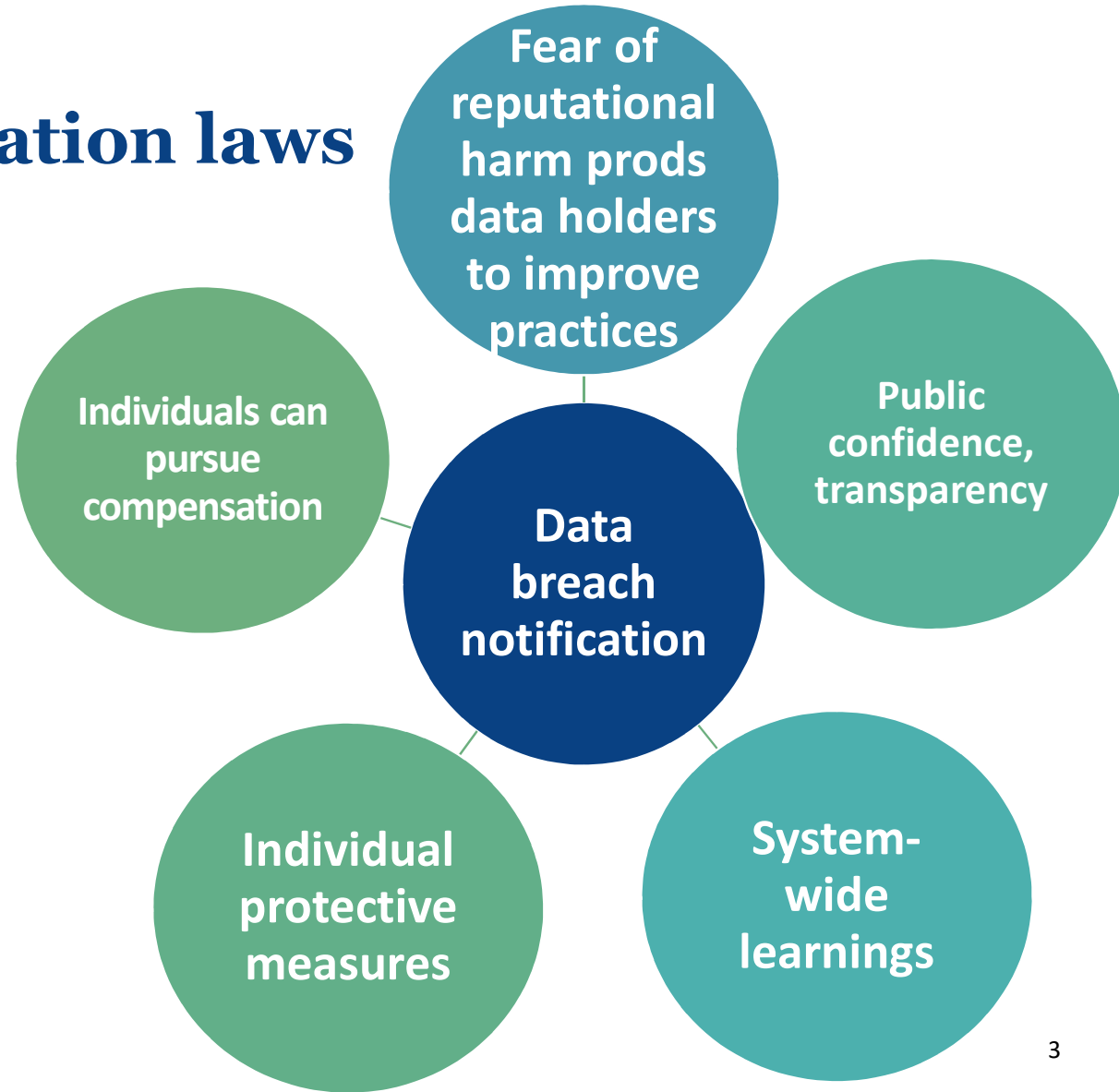
A study of figures from the Information Commissioner's Office (ICO) by data security firm Egress found that human error, rather than external threats, was the main cause of breaches across every sector of the UK economy.

Healthcare organisations suffered 2,447 data breaches and accounted for 43 per cent of all reported incidents between January 2014 and December 2016. Cumulative healthcare breach numbers were almost four times more than the second highest sector, local government.



Data breach notification laws

- Telling people affected by a data breach, that their information has been lost or subject to unauthorised access or disclosure
- Enshrined in law in Aus, EU, US
- How might notification address the problem of data breach?





Australia: data breach notification laws

- Notifiable Data Breaches Scheme – in the *Privacy Act 1988* (Cth) Part IIIC
 - Federal government agencies, private companies including healthcare providers: hospitals, GPs, specialists, business and non-profits.
 - NOT public hospitals nor research institutions at state level.
 - *Unauthorised access/loss/disclosure AND*
 - *Likely to result in serious harm AND*
 - *Data holder can't remediate the harm*
- Must notify (but 30 days to investigate first)*
- Maximum penalty for failure to notify: \$2.1 million*
- *My Health Records Act 2012* (Cth) ALL healthcare providers - MHR data only
 - No comparable state-based legislation



Europe: Notifiable data breach under GDPR

- Notify supervisory authority <72 hours after becoming aware of breach (Article 33)
 - Nature of breach
 - Likely consequences
 - Steps taken to mitigate
- If there is a high risk breach will adversely affect individuals' rights and freedoms – notify them 'without undue delay' (Article 34)
- Penalties for failure to notify:
 - fines: up to €20 million or 4 percent of global revenue
 - cessation of data processing operations with EU members



Where to from here?

- If your organisation holds personal data – consider policies and practices
- More information: see OAIC website
- Lagging behind: Europe has more stringent notification requirements, shorter timelines, higher penalties.
- Conceptual development: which are the most important goals of data breach notification and how can we shape laws to achieve these?
- Law reform opportunities: state-based laws mirroring Cth scheme so that universities and public hospitals must notify.



Megan Prictor
megan.prictor@unimelb.edu.au

**Health, Law and Emerging Technologies team,
Melbourne Law School
law.unimelb.edu.au/helex**

