Emerging Risk Privacy Breaches

Angela Mason-Lynch
Risk Adviser

Privacy breaches

> Email / Mail

> SMS and Mobile

> Data checking

> Vexatious receptionist behaviour

> Vexatious patient behaviour

> Cyber

We are the independent national regulator for privacy and freedom of information. We promote and uphold your rights to access government-held information and have your personal information protected.

Angelene Falk is the Australian Information Commissioner and Privacy Commissioner.

Make a privacy complaint →

Report a data breach →

Apply for an FOI review →

ⓘ Read our new Australian Community Attitudes to Privacy Survey   Updated 2 October 2020

hccc
HEALTH CARE
COMPLAINTS
COMMISSION

Home | About us | Understanding Complaints | Health Consumers | Health Providers | Decisions & Orders | Contact us

Committed to protecting public health and safety

We deal with complaints about health service providers in NSW.

Make a complaint

or call 1800 043 159 for further information.

⊙ **COVID-19 information**

Legislative amendments to powers and functions of the Commission

▌▌ How can we help you?

Do I have a complaint?
›

I need to make a complaint
›

A complaint has been made about me
›

Check my practitioner
›

Poll Question

> Have you ever had to notify that there has been a data breach

       A. to the patient
       B. to the Privacy Commission
       C. to both of the above
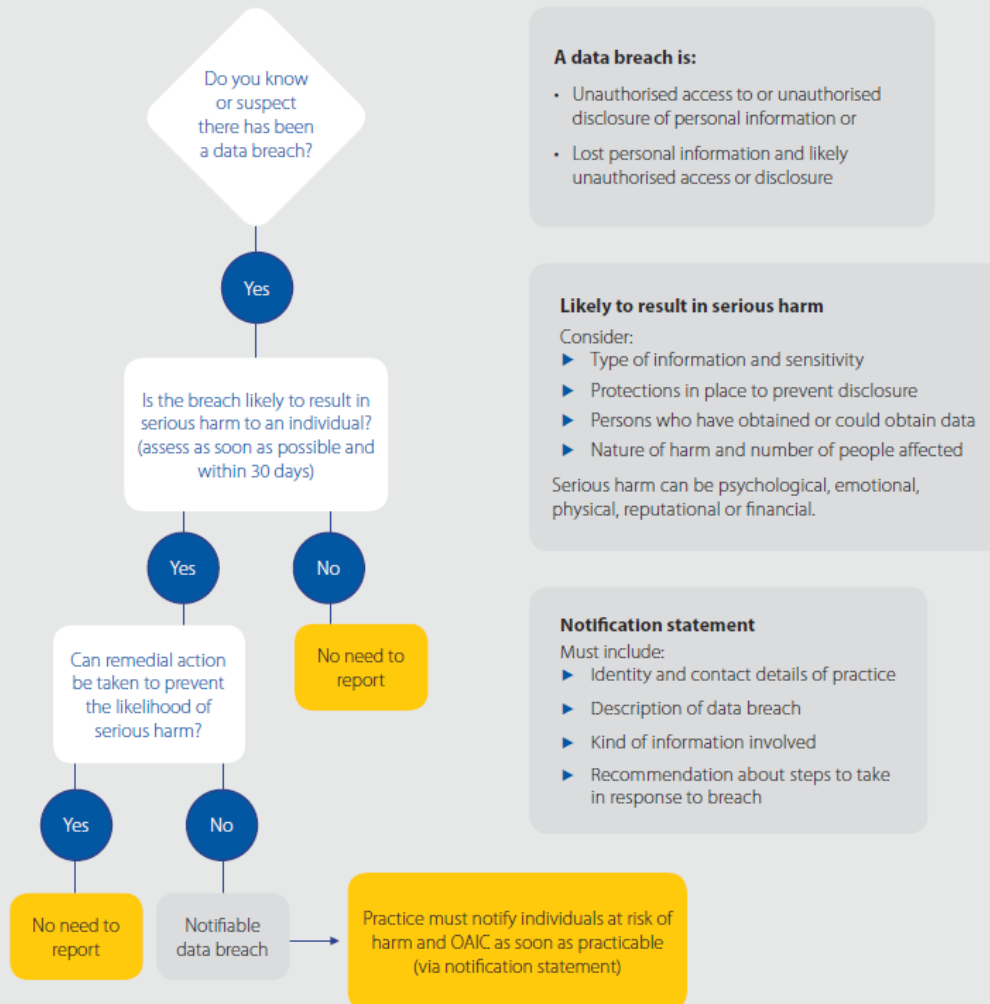   D. never had to notify

PRIVACY BREACH case study

Questions:

When do you have to notify and what does that mean?

What evidence will you be able to produce if you do have a claim / notify?

Notifiable Data Breach Scheme

From 22 February 2018, organisations covered by the Privacy Act 1988 are required to notify individuals likely to be at risk of serious harm because of a data breach, and to notify the Office of the Australian Information Commissioner. Use the decision-making flowchart to assist you to determine whether to report a breach.

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

Yes

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

Yes

No

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

No need to report

Yes

No

No need to report

Notifiable data breach

Practice must notify individuals at risk of harm and OAIC as soon as practicable (via notification statement)

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

Email / Facsimile / Mail

- Who can send
- What can be sent
- Who can it be sent to
- Address confirmation
- Consent confirmation
- Identify patient
- Document
- Defence building blocks – written system / training

STOP!!!!

Consent – pt or third party

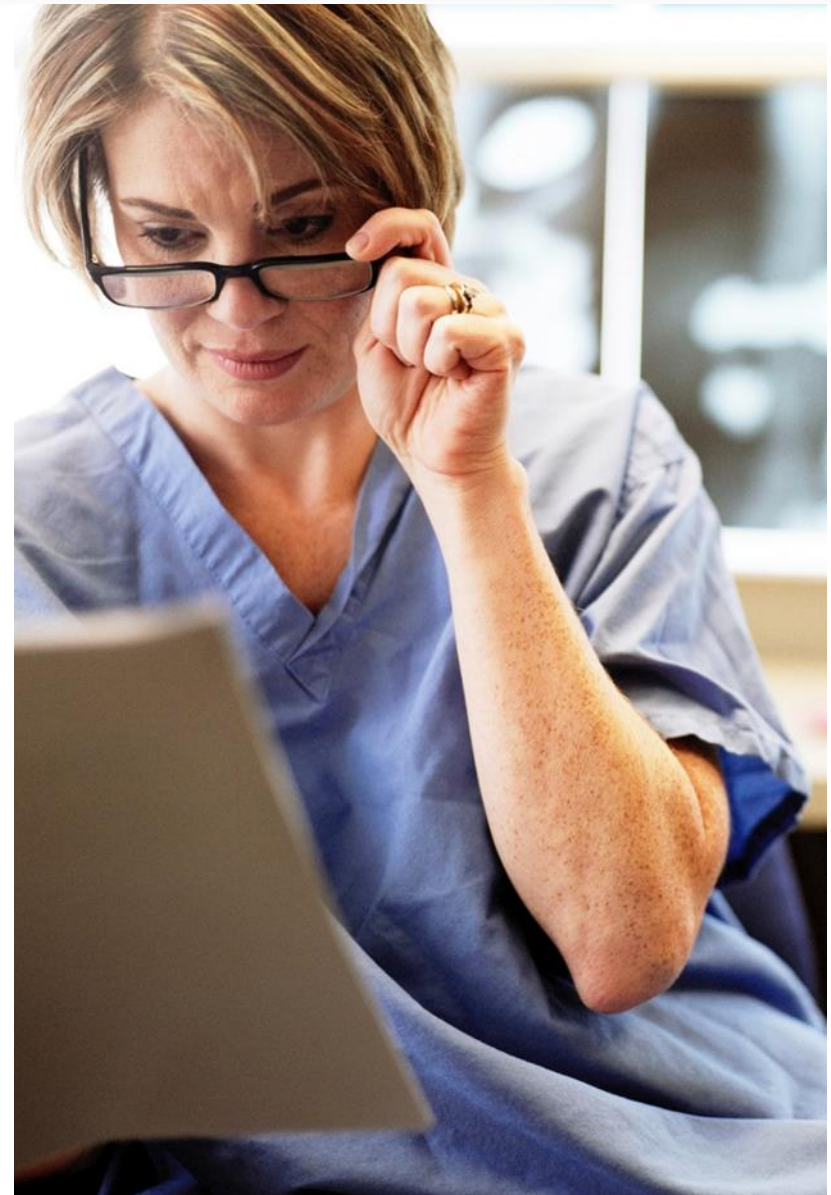**A**ddress – pt or third party

Name, DOB Address - all pages

Document

Ongoing review

SMS Communication

> Consent

> Security at the receiving end

> What is sent

> Alert receptionists

Data Checking

Name, DOB, Address, ? Telephone

- Ask don't tell
- Photo identification
- Pt entry
- Paper form

Vexatious Behaviours

- Evidence of training
- Evidence systems
- Confidentiality statements
- Privacy Policy

Cyber attack

Information security in general practice

Prevention
Protection
Preservation

> Security confirmation (RACGP Information Security Guidelines)

https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/introduction

> Confirmation from IT support

> Backup taken off site and away from server

> Cloud security confirmation

> Restore from backup performed

Poll Question

> Should you have notified a data breach?

 A. to the patient
 B. to the Privacy Commission
 C. to both of the above
 D. never had to notify

Take Home Message

- Document your systems
- Train your team and keep evidence
- Know your systems and how they work
- Review what your people are doing
- Think before you send / fax / post
- Its very easy to complain
- What you do reflects the credibility of your practice
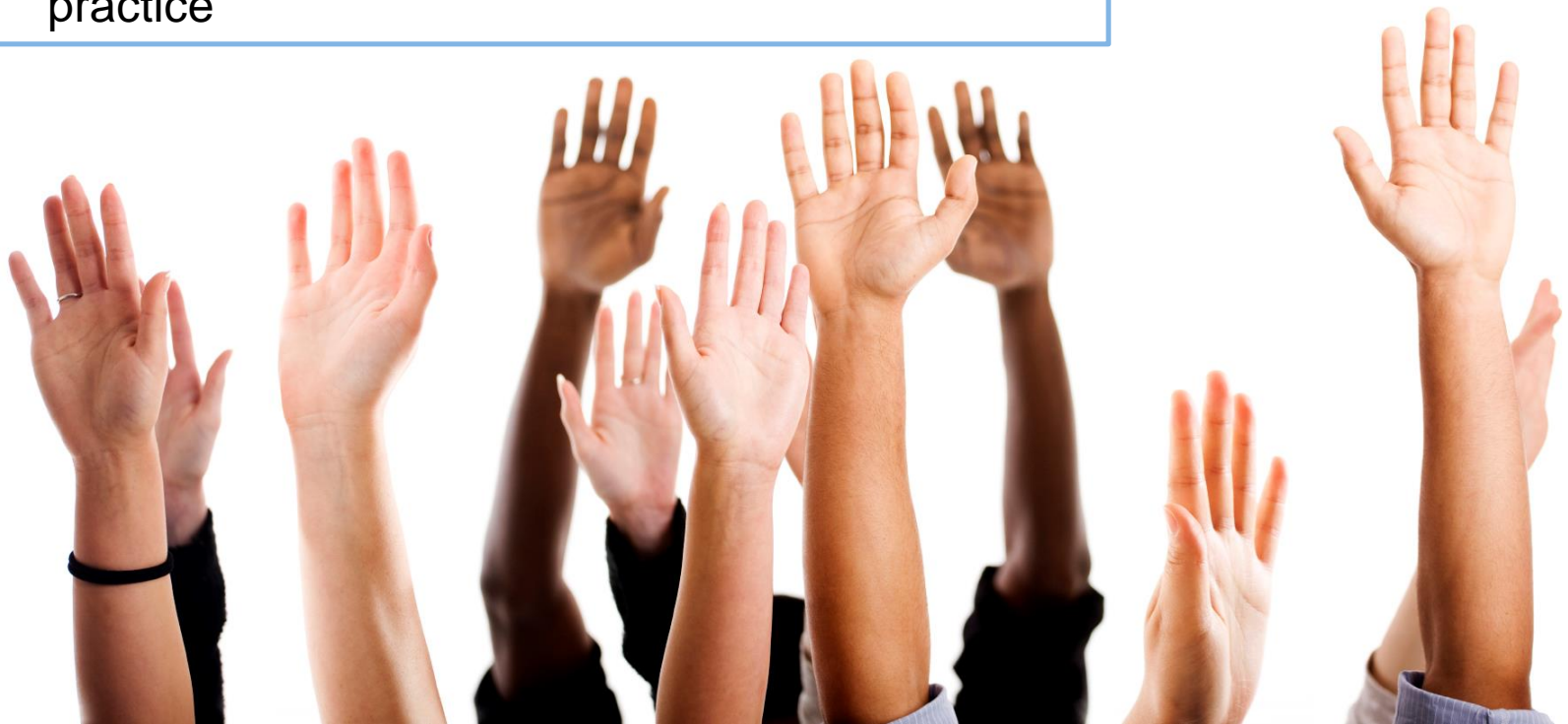
Avant Medico-legal Advisory Service: 1800 128 268