



New territory for privacy and security laws

Annabel Herron- Risk Adviser
AVANT



ASA Practice Managers Conference 2017



Why Privacy?



The charming simplicity
of Australian privacy law

Source: <http://www.sangrea.net/free-cartoons/privacy-cartoons.html>

Australian
Doctor.

GPs face huge fines over PCEHR privacy breaches

Paul Smith | 16 October, 2015 | **23 comments** [Read Later](#)

GPs and practice staff face jail and fines of up to \$108,000 for misuse of the PCEHR system under controversial new laws being pushed through the Federal Parliament.

Audit of GP clinics flags patient privacy risks

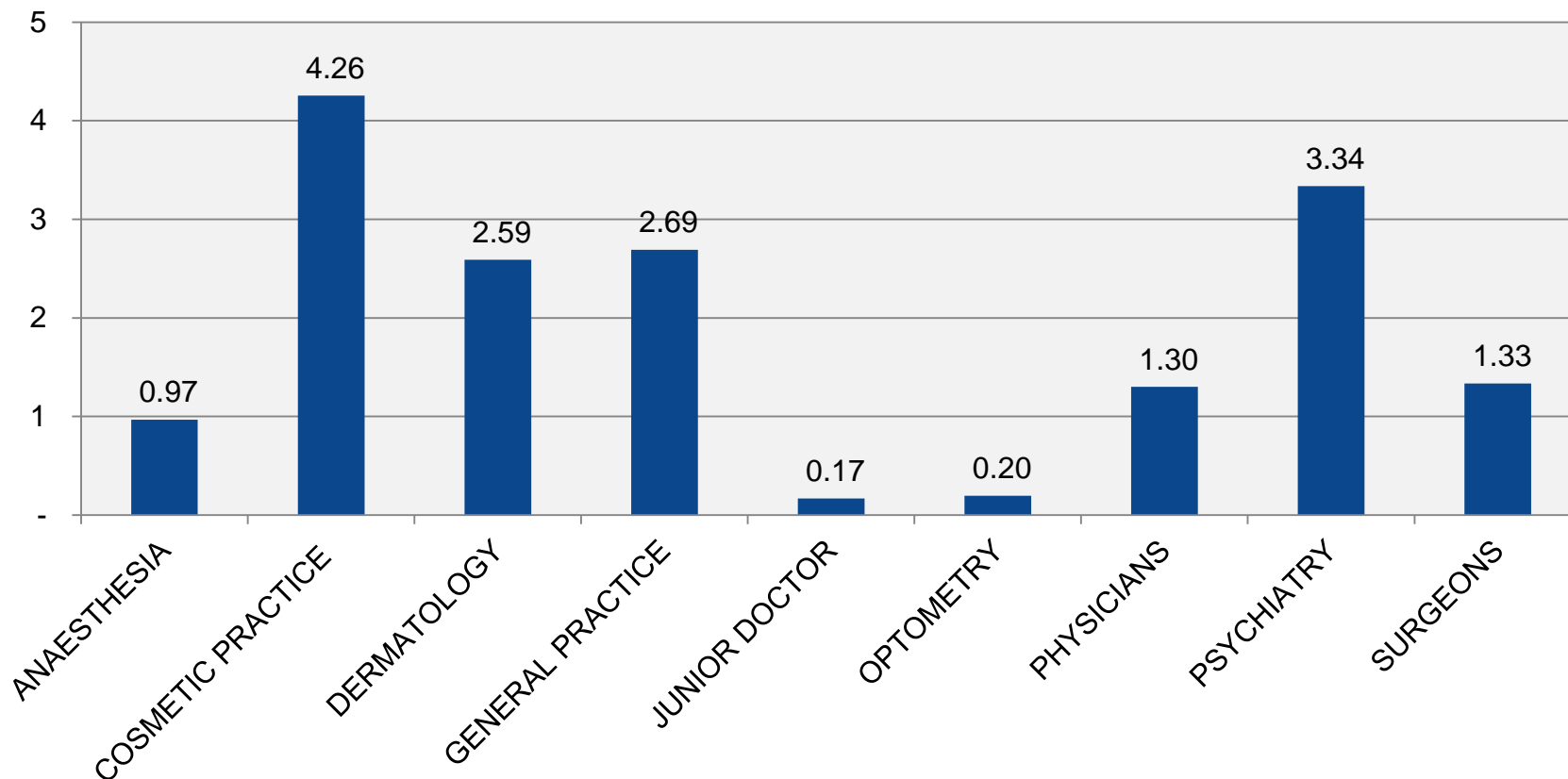
Tessa Hoffman | 19 November, 2015 | **0 comments** [Read Later](#)

Lax security measures in GP clinics are putting patients' electronic records at risk of privacy breaches, a government audit has found.

Source: <http://www.australiandoctor.com.au/home>

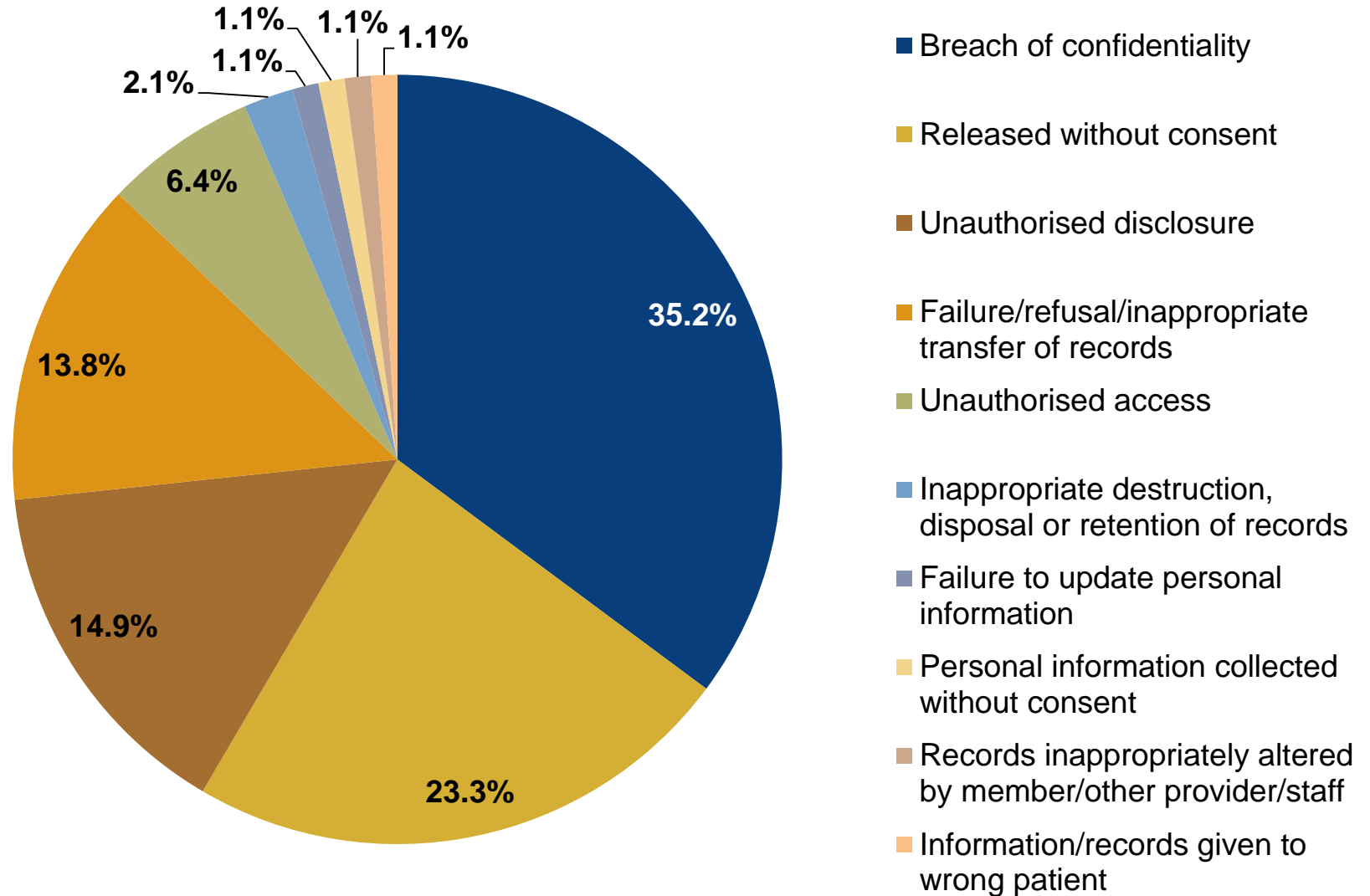
Frequency of privacy claims by speciality

Ratio of proportion of claims to proportion of members



GPs and GP registrars make up the majority (65%) of privacy claims

Breakdown of privacy claims



2% of Avant claims relate to Privacy

History of the Privacy Act



Confidential

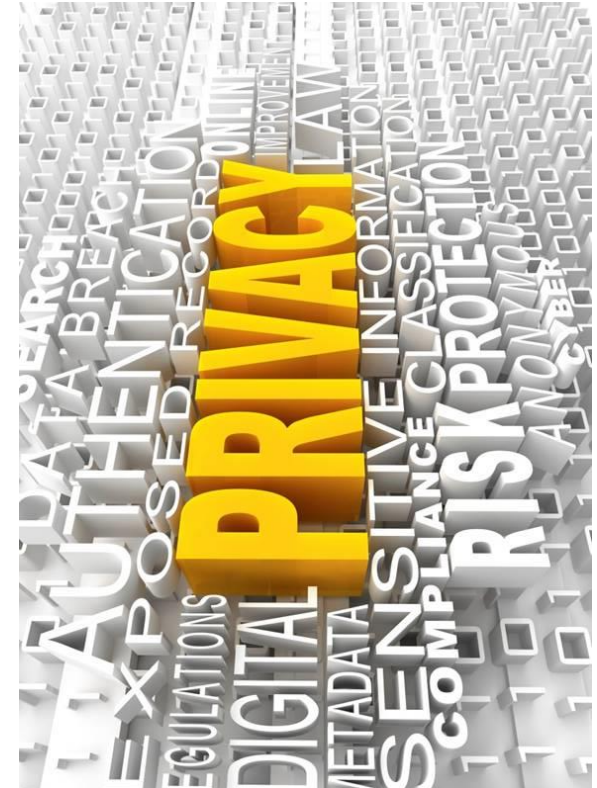
Privacy Act was enacted in 1988 and extended to the private sector in December 2001

Applies to all health service organisations


Most information collected and used by health practices will be considered as 'sensitive information' and subject to more stringent protection under the Act

Changes from 12 March 2014

- Thirteen new Australian Privacy Principles for both the private and government sectors.
- Requirements for all health services to have a privacy policy.
- Health information transferred overseas must comply with the APPs.
- Greater restrictions on the use and disclosure of personal information for direct marketing purposes.
- Greater investigation powers by the Privacy Commissioner
- Enhanced enforcement powers and penalties: civil penalty orders of up to \$340K for individuals and up to \$1.7m for corporations for serious interference or repeated breaches of privacy.



New changes



From 22 February 2018*
Mandatory obligation to notify individuals who may be affected by
an eligible data breach

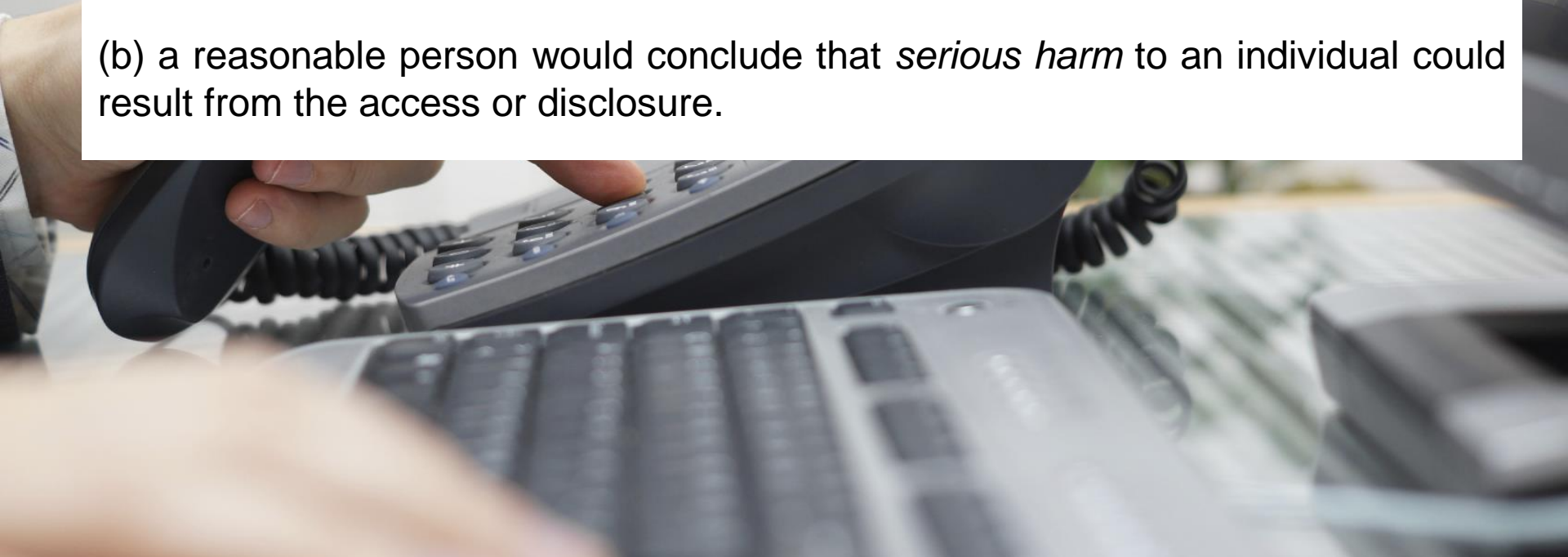
**Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)*

What is an 'eligible data breach'?

(a) either:

- i. there is unauthorised access to, or unauthorised disclosure of, information held by a health provider; or
- ii. information is lost in circumstances where there is likely to be unauthorised access to or unauthorised disclosure of information; and

(b) a reasonable person would conclude that *serious harm* to an individual could result from the access or disclosure.



What is not an 'eligible data breach'?

If an entity takes remedial action:

- (a) prior to any serious harm occurring from a data breach
- (b) prior to any unauthorised disclosure, access or loss of information
- (c) after information is lost, accessed or disclosed, but before that access or disclosure results in any serious harm to an individual



What is 'serious harm'?



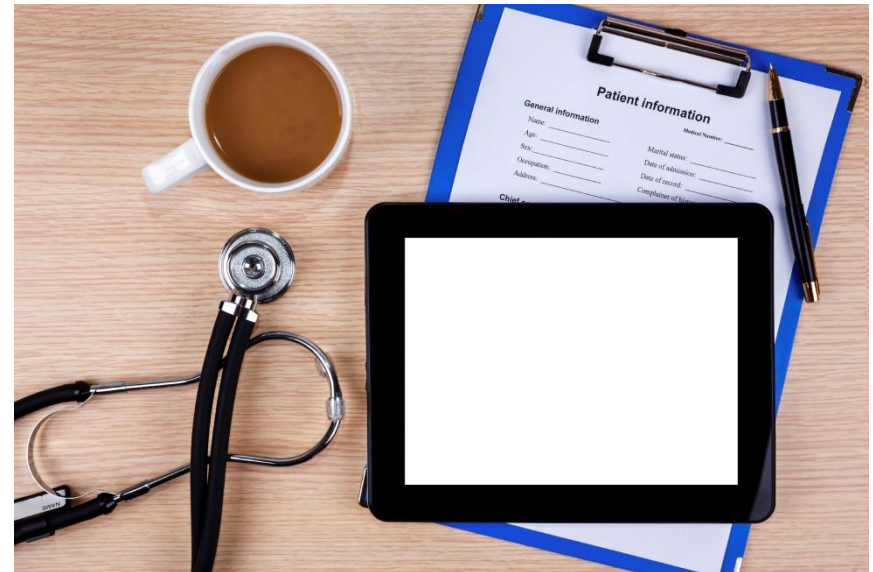
Serious harm 'could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach'.

Explanatory Memorandum to the Act

Requirement to assess

If a health provider suspects that a data breach has occurred, then they must:

1. Investigate whether it is an eligible data breach
2. Complete the investigation within 30 days



Requirement to notify the OAIC

Health provider must provide a report to the Office of the Australian Information Commissioner (OAIC):

1. As soon as becoming aware of an eligible data breach; or
2. If requested to do so by the Commissioner.

The report must set out:

- i. Identity of the health provider; and
- ii. Description of the breach; and
- iii. Nature of the information that was lost, accessed or disclosed; and
- iv. Steps that an individual could take in response to the data breach (to protect themselves from further harm)

Requirement to notify affected individuals

Health provider must make available a copy of any report prepared for the Commissioner:

1. To individuals actually affected
2. To individuals who might be at risk of being harmed
3. Online if individuals cannot be identified



Penalties for 'eligible data breaches'

The Office of the Australian Information Commissioner (OAIC) can:

- > Impose penalties: such as public or personal apologies, compensation payments or enforceable undertakings.
- > Refer serious or repeated breaches to the Federal Court, which can impose financial penalties.



Case Study

Case study – accessing records



Your privacy policy

Explains to the general public:

- How your practice handles a patients personal information.
- The kind of personal information you collect.
- Purposes of handling personal information.
- Who you may disclose it to and how.
- How individuals can access and seek correction of their health record.
- How they can make a privacy complaint.



Case study – content to share



Case History Form

Patient Name - Last	First	Middle Initial	Date of birth	Age	Sex
Address - Number, Street		City, ZIP		State	
Ethnicity					

PRESENT ILLNESS

Onset date	Hospitalized? Yes <input type="checkbox"/> No <input type="checkbox"/>	Admit date	Hospital Name
Level of medical care (check all that apply): <input type="checkbox"/> Outpatient clinic <input type="checkbox"/> Emergency Room <input type="checkbox"/> Inpatient ward <input type="checkbox"/> Intensive Care Unit <input type="checkbox"/> None		Significant past medical history:	
Symptoms that occurred during the current illness (check all that apply): <input type="checkbox"/> Fever (≥ 38 °C) <input type="checkbox"/> Seizures <input type="checkbox"/> Ataxia <input type="checkbox"/> Nausea <input type="checkbox"/> Vomiting <input type="checkbox"/> Altered consciousness <input type="checkbox"/> Lower respiratory (cough, wheezing, shortness of breath, bronchospasm) <input type="checkbox"/> Other:		Cardiac disease..... Chronic pulmonary disorder (e.g. Asthma, cystic fibrosis)..... Infectious disease (e.g. Hepatitis, HIV)..... Immunosuppression (e.g. HIV, malignancy)..... Neuromuscular disorder..... Metabolic Disorder (e.g. diabetes mellitus, renal)..... Spinal disorder..... Ear, nose, throat..... Hypertension..... Long-term aspirin therapy..... Diastolic therapy..... Cancer chemotherapy..... Radiation therapy..... Other immunosuppressive medications..... Previous..... If Yes, specify number of weeks.....	
Medicine received and why:			

Case study - correcting records



Amendment of medical records is an obligation of the organisation if they are:

- inaccurate
- out of date
- incomplete
- misleading or
- if a patient says that it is incorrect. You are not obliged to correct it if the practice believes it is correct.

Withholding of medical records is allowed if:

- you believe that access would pose a serious threat to life or health of an individual
- it would breach an individual's privacy
- legally deny access based on an equitable duty of confidentiality for part or all of the record.

Case study – security of records

Do you drink alcohol?
Do you take drugs?

Marital Status: Married

Single

Divorced

Employment: (Type) _____

FAMILY HISTORY (Siblings, parents)

No Diseases

Asthma

Arthritis

Cancer

Diabetes

High Blood Pressure

Kidney Disease

Prostate Disease

Seizure

Stroke

Tuberculosis

Anesthesia

Bleeding



Case study - Police access to records



PRIVACY

The word "PRIVACY" is written in large, bold, white capital letters. The letter "V" is highlighted in orange. The text is centered over a blue background featuring several white gears of various sizes. In the background, there are faint, blue silhouettes of people, suggesting a medical or professional setting.

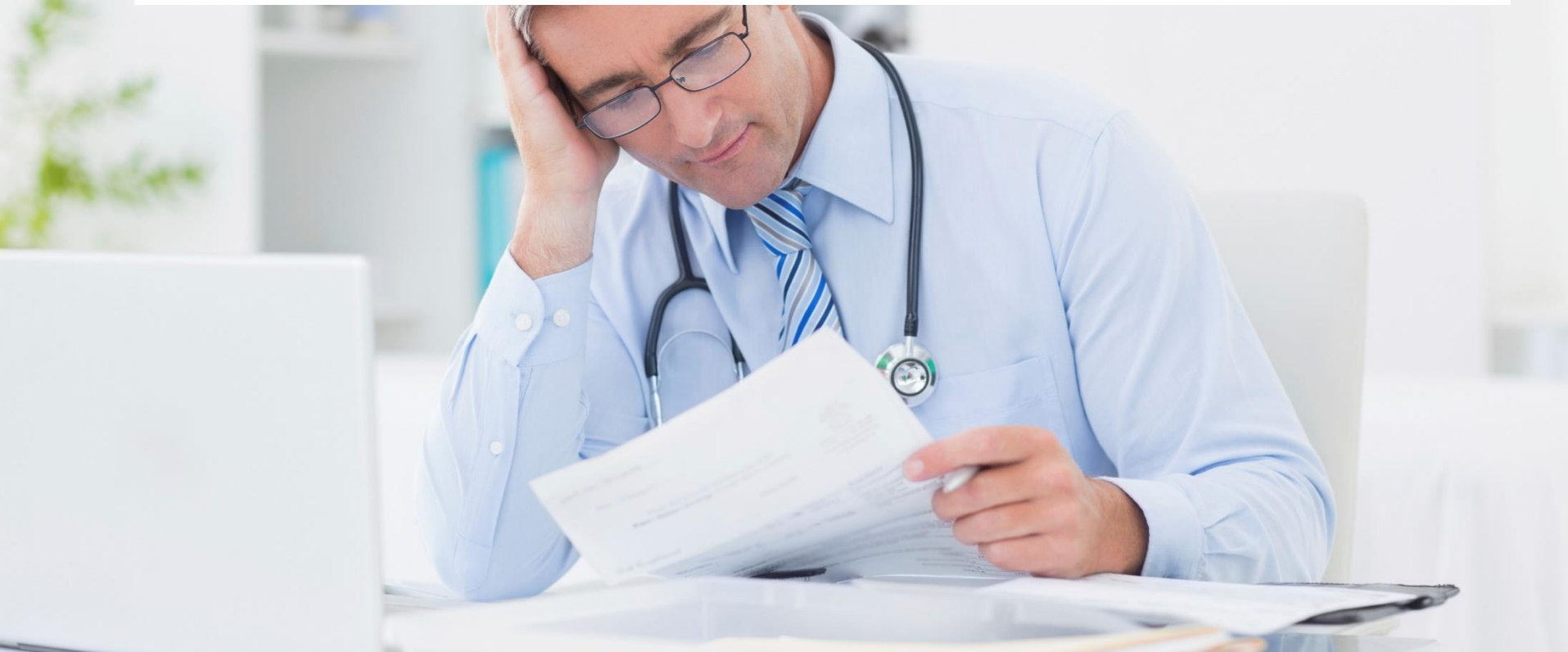
Preparing for the changes: What should you do?

Transition process

1. Review and update privacy policies and procedures.
2. Create a detailed data breach response plan.

The OAIC provides guidelines to help, including:

Data breach notification - A guide to handling personal information security breaches and Guide to developing a data breach response plan.

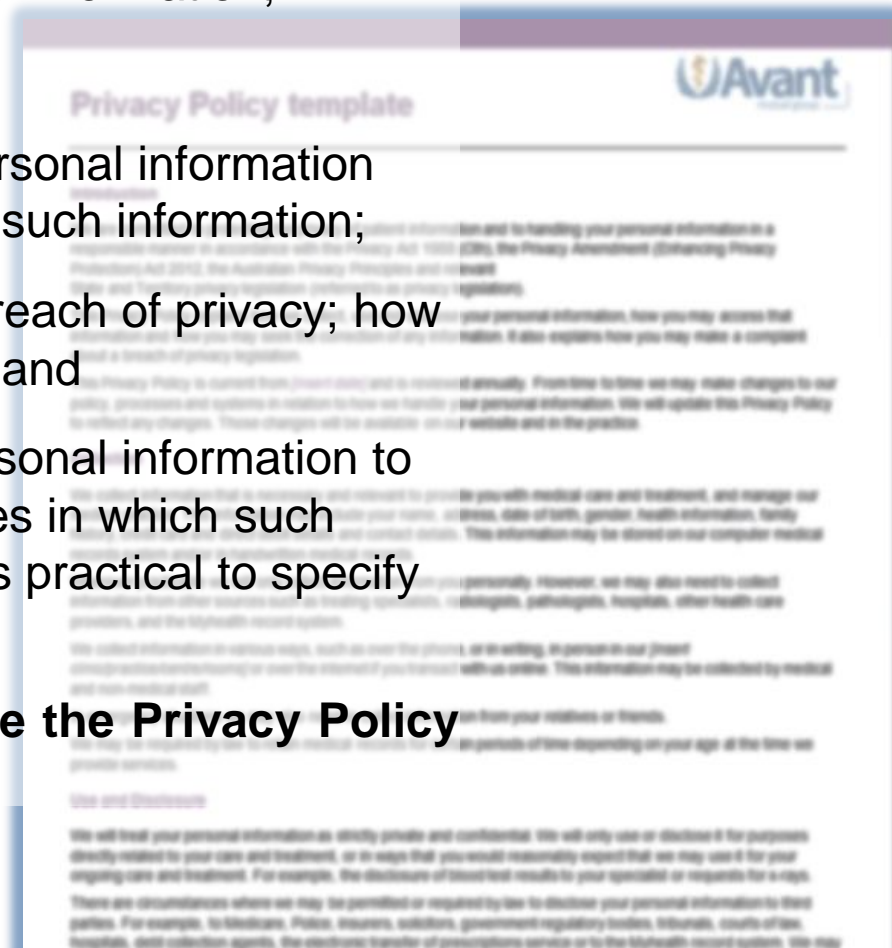


Privacy policy contents


The privacy policy must contain information about:

- > the kind of personal information the entity collects;
- > how the entity collects and holds personal information;
- > the purpose of collection;
- > how an individual may seek access to personal information held by the entity or to seek correction of such information;
- > how a complaint may be made about a breach of privacy; how the entity will deal with such a complaint; and
- > whether the entity is likely to disclose personal information to overseas recipients and if so, the countries in which such recipients are likely to be located and if its practical to specify those countries.

Reasonable steps must be taken to make the Privacy Policy available to patients free of charge.



Privacy policy – accreditation requirements



‘our practice team can demonstrate how patients are informed about our practice’s policy regarding management of their personal health information’

Australian **Doctor.**

[Home](#) / [News](#) / [Latest News](#) /

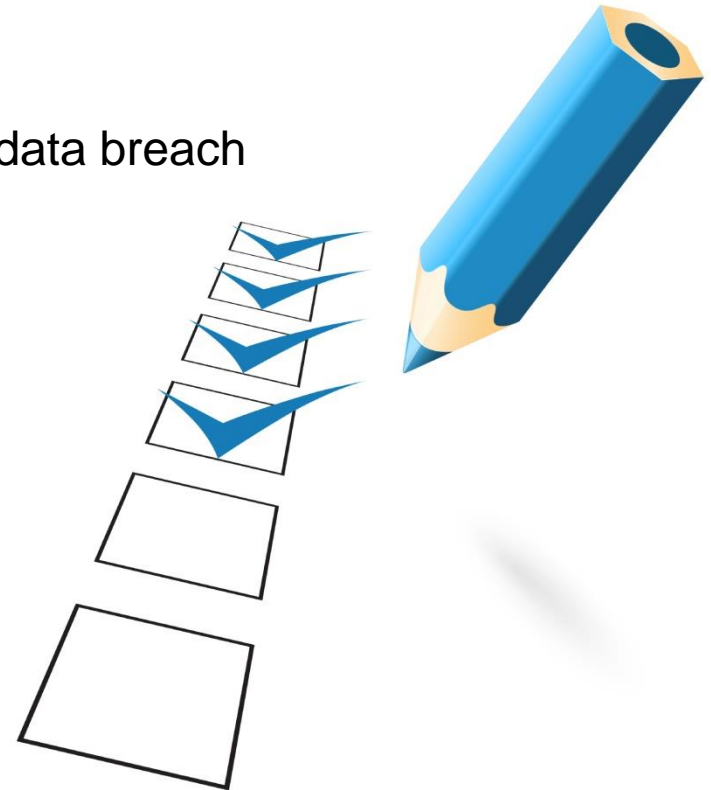


1500 specialist letters, meant for referring GPs, found in suburban bin

Antony Scholefield | 21 April, 2017 | [5 comments](#) [Read Later](#)

Data breach response plan checklist

- ✓ Written policy
- ✓ Educate staff
 - about the policy
 - what to do if they know of or suspect a data breach
- ✓ Regularly review and test the plan
- ✓ Dedicated staff and resources
- ✓ Establish a data response team
 - team leader
 - legal support
 - clear reporting lines
- ✓ Communication strategy
 - media
 - affected individuals
 - OAIC
- ✓ Seek advice (Avant or your insurer)



Questions?



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 document.