

This is an extremely important code of ethical behaviour and must be maintained at all times by all staff. The legal requirements of confidentiality extends from the practice principals, Practice Manager and to all clinicians and practice staff.

VERBAL BREACH of confidence - Discussion of patient's conditions with staff members, families, friends and others.

VISUAL BREACH of confidence - Leaving patient's records in full view of any other party.

AUDITORY BREACH of confidence - Discussing patient matters (in hearing range of other's nearby).

Policy

The practice recognises that prevention of data breaches is much better than dealing with them after the fact. This policy also supports the practice's other obligations under the Privacy Act.

Organisations covered by the Privacy Act have obligations under the Act to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

A data breach is:

- Unauthorised access to or unauthorised disclosure of personal information, or
- Lost personal information and likely unauthorised access or disclosure

Examples of a data breach include an email sent to the wrong person, a lost laptop containing patient information or your database being hacked.

If a breach has occurred, the practice will consider if the breach is likely to result in serious harm to an individual.

For '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
- Financial

The practice has a data breach response plan that helps establish robust and effective procedures in the event of a data breach. The purpose of the plan is to ensure that quick actions can be taken after discovering a data breach.

A data breach response plan is a framework which sets out the roles and responsibilities for managing an appropriate response to a data breach as well as describing the steps to be taken by the practice in managing a breach if one occurs. This includes:

- the members of the data breach response team (response team)
- the actions to be taken if a breach is suspected, discovered or reported by a staff member or other person, including when it is to be escalated to the response team
- the actions the response team is expected to take.

The plan clearly identifies those actions that are legislative or contractual requirements.

The purpose of a response team is to ensure that the relevant staff, roles and responsibilities are identified and documented before the data breach happens.

All staff is aware of the plan, response team members and clearly understands what needs to happen in the event of a data breach.

The plan is regularly reviewed and tested including simulating the practice's response to a hypothetical data breach

Procedure

The practice has a data breach response team. The data breach response team consists of:

- Practice Manager
- Practice Principals
- GravIT (if applicable)
- Indemnity Insurance Agency (AVANT)

All members of the practice team are aware of the actions to be taken if a breach is suspected, discovered or reported by any staff member.

The data breach response team is informed of **any** potential breaches. The team should be informed as soon as a breach or potential breach is identified. The team should be informed verbally if a team member is available, or via email if the team members are not on site.

In the event of a breach, the response team will gather and document all available details about the nature of the breach, including any technological aspects of the breach, timing, duration and format. This might include:

- details of person/organisation reporting the potential breach –
- what action they claim to have taken in response to the situation (e.g. email or fax received by mistake; discovery of sensitive information online etc.);
- forensic analysis of data access or information transfer in the event of unauthorised database/system access; analysing CCTV footage, possibly contacting relevant police or security services.

Once this process has been undertaken or commenced, the practice could contact the practitioners'/practice's medical defence organisation for advice and notification.

The response team will:

- assess if the breach is likely to result in serious harm to an individual/individuals with assessment to occur as soon as possible and within thirty (30) days
- where possible, undertake remedial action to prevent the likelihood of serious harm
- depending on the size and nature of the data breach, decide the most appropriate form of contacting affected individuals, or individuals potentially affected by the breach (e.g. individual phone calls, emails, written letter, newspaper advertisement, signage in the practice etc.)
- contacts the individuals at risk of harm and Office of the Australian Information Commissioner (OAIC) as soon as practicable, if it is not possible to take remedial action

The response team will also consider:

1. If the breach or suspected breach indicate a systemic problem with the practice's or procedures.
2. Strategies to identify and address any weaknesses in data handling that contributed to the breach
3. Other issues relevant to the practice's circumstances, such as the value of the data to the practice or issues of reputational risk
4. A system for a post-breach review and assessment of the practice's response to the data breach and the effectiveness of the data breach response plan.

Additional Information about the 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 from serious harm because of a data breach, and to notify the Office of the Australian Information Commissioner (OAIC).

Helpful resources:

[Privacy basics and data breaches](#) (Avant 08/11/2017)

[New privacy laws coming into force – are you ready?](#) (Avant 23/10/2017)

[Guide to developing a data breach response plan](#) (OAIC April 2016)

[Notifiable Data Breach Scheme Decision Making Flowchart](#) (Avant October 2017)

[RACGP Computer and Information Security Standards Data incident/breach report](#)

[Notifying individuals about an eligible data breach](#) (OAIC December 2017)

[Preventing data breaches](#) (Avant 01/02/2018)

[OAIC Data breach notification guide: A guide to handling personal information security breaches](#)

The Privacy Act

The [Privacy Amendment \(Sector\) Act 2000](#) extends the operation of the Privacy Act 1988 to cover the private health sector throughout Australia.

The Privacy Act requires our practice to abide by the 13 Australian Privacy Principles (APPs):

- a. [APP 1 – open and transparent management of personal information](#)
- b. [APP 2 – anonymity and pseudonymity](#)
- c. [APP 3 – collection of solicited personal information](#)
- d. [APP 4 – dealing with unsolicited personal information](#)
- e. [APP 5 – notification of the collection of personal information](#)
- f. [APP 6 – use and disclosure of personal information](#)
- g. [APP 7 – direct marketing](#)
- h. [APP 8 – cross-border disclosures](#)
- i. [APP 9 – adoption, use or disclosure of government related identifiers](#)
- j. [APP 10 – quality of personal information](#)
- k. [APP 11 – security of personal information](#)
- l. [APP 12 – access to personal information](#)
- m. [APP 13 – correction of personal information](#)

Resources:

Information regarding complying with the legislation is available at the [Office of the Australian Information Commissioner](#)

The RACGP's Privacy and managing health information in general practice at www.racgp.org.au/your-practice/ehealth/protecting-information/privacy

[Privacy Policies for GPs](#) (OAIC August 2015)