

»  
**aitken**  
partners



# PRIVACY 2023

23 FEBRUARY 2023  
BUSINESS LAW BREAKFAST

# PRIVACY 2023



**Julie Maxfield**

Principal

Aitken Partners

(03) 8600 6045

[jmaxfield@aitken.com.au](mailto:jmaxfield@aitken.com.au)



**Ric Birkett**

Principal Lawyer

Aitken Partners

(03) 8600 6005

[rbirkett@aitken.com.au](mailto:rbirkett@aitken.com.au)



**Bhrig Chauhan**

Principal Lawyer

Aitken Partners

(03) 8600 6019

[bchauhan@aitken.com.au](mailto:bchauhan@aitken.com.au)



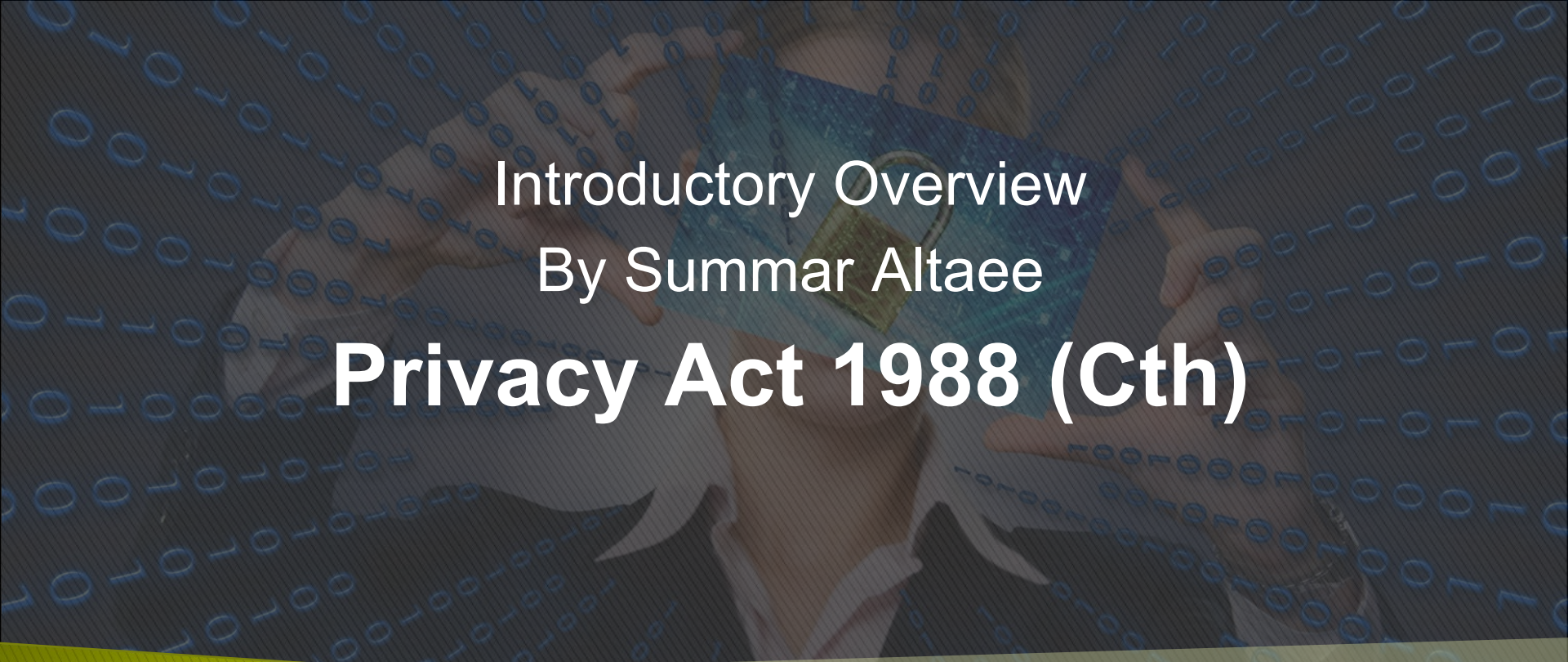
**Summar Altaee**

Associate

Aitken Partners

(03) 8600 6069

[saltaee@aitken.com.au](mailto:saltaee@aitken.com.au)



Introductory Overview  
By Summar Altaee  
**Privacy Act 1988 (Cth)**



[aitken.com.au](http://aitken.com.au)



[@aussie\\_lawyer](https://twitter.com/aussie_lawyer)



[/company/aitken-partners](https://www.linkedin.com/company/aitken-partners)

**aitken**  
partners

# The Privacy Act

- » What does it regulate?
- » Why is it important?

# What is Personal Information?

- » Information or an opinion about an identified individual, or an individual who is reasonably identifiable:
  - whether the information or opinion is true or not; and
  - whether the information or opinion is recorded in a material form or not.
- » General consensus is that it can include:
  - Name, address, phone number
  - Date of birth
  - Medical records

# What is Personal Information?

- » Other *types* of information recognised as constituting personal information:
  - Sensitive information
  - Health information
  - Credit information
  - Employee record
  - Tax file number information

# Australian Privacy Principles (“APP”)

- » An APP entity must not do an act, or engage in a practice, that breaches an APP (s 15).
- » An act or practice breaches an APP if, and only if, it is contrary to, or inconsistent with, that principle. (s 6A)
- » APPs extend to an act done, or practice engaged in, outside Australia and the external Territories by an organisation, or small business operator, that has an Australian link (s 5B(1A)).

# What is an APP entity?

- » An APP entity is defined as an
  - ‘agency’ or
  - ‘organisation’



# What is an agency?

» An agency is:

- a Minister; or
- a Department; or
- a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment....

NB the above list is not exhaustive, and there are exceptions

# What is an organisation?

» An Organisation means:

- a) an individual; or
- b) a body corporate; or
- c) a partnership; or
- d) any other unincorporated association; or
- e) a trust.

that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

(see s 6C)

# What is a small business?

- » A business is a “small business” at a time (the test time) in a financial year (the current year) if its annual turnover for the previous financial year is \$3,000,000 or less.
- » Test for new business – however, if there was no time in the previous financial year when the business was carried on, the business is a small business at the test time only if its annual turnover for the current year is \$3,000,000 or less.

# What is a small business operator?

- » A “small business operator” is an individual, body corporate, partnership, unincorporated association or trust that:
  - a) carries on **one or more small businesses**; and
  - b) does not carry on a business that is ***not a small business***.

# What is not a small business operator?

1. carries on a business that has had an annual turnover of more than \$3,000,000...; or
2. provides a health service and hold any health information...; or
3. discloses personal information to anyone...; or
4. provide a benefit, service or advantage to collect personal information ...; or
5. contracted service provider for a Commonwealth contract...; or
6. credit reporting body.

# What do APPs deal with?

- » Privacy of personal information
- » Collection of personal information
- » Dealing with personal information and government related identifiers
- » Integrity of personal information
- » Requests for access and the correction of personal information

# What are the APPs?

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing

# What are the APPs?

8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information



# Privacy Policy

- » APP entity must have a clearly expressed and up to date privacy policy.
- » The specific requirements for an APP privacy policy are further set out in APP1, and include:
  - the topics an APP privacy policy must cover (APP 1.4);
  - a requirement for an APP entity to take reasonable steps to make the privacy policy available free of charge and in an appropriate format (APP 1.5); and
  - a requirement for an APP entity to take reasonable steps to give its privacy policy to an individual in the form the individual asks for (APP 1.6).

# Considerations for Privacy Policy

- » The specific needs and requirements of your business.
- » Your entity's main functions and activities.
- » What kinds of personal information does your company collect and hold?
- » How is the personal information managed by your organisation/employees?
- » Access to a party's personal information.
- » How to make a complaint and how that complaint will be dealt with.
- » The policy should be user friendly, easy to read and understandable for the clients of your business

# Employee Training

- » APP 1.2 requires an APP entity to take such steps to implement practices, procedures and systems to ensure that the entity complies with the APP's and that will enable the entity to deal with inquiries or complaints from individuals.
- » To comply with this principle, all employees of an entity that handle personal information should be trained to avoid privacy risks and promote trust and confidence in your business.

# Employee Training

- » Importance of keeping personal information secure.
- » Responding to customer queries about collection of personal information (whether that be identity information or TFN's).
- » Dealing with complaints.
- » Informing customers how your business keeps their information secure and the relevant policies for storage and destruction of that information.

# Collection of Personal Information other than sensitive information

- » An agency must not collect personal information (other than sensitive information) unless reasonably necessary or directly related to its functions or activities (APP 3.1).
- » An organisation must not collect personal information (other than sensitive information) unless it is reasonably necessary for one or more of the entity's functions or activities (APP 3.2 ).

# Collection of sensitive information

- » An APP entity must not collect sensitive information unless the individual consents and
  - APPs 3.1 (for agency) or 3.2 (for organisation) have been satisfied (APP 3.3); or
  - the exemptions under APP 3.4 apply.
  - (see APP 3.3)
- » An entity must collect personal information only by lawful and fair means (APP 3.5 ).

# Means of collection

- » Only by lawful and fair means (APP 3.5)
- » Only from the individual unless (APP 3.6):
  - a) if the entity is an agency:
    - i. with consent; or
    - ii. as required or authorised by law, or a court/tribunal order; or
  - b) it is unreasonable or impracticable to do so.
- » APP 3 applies only to the collection of personal information that is solicited by an APP entity.
- » For unsolicited personal information, see details under PPA 4.

# Notification of collection of personal information

- » At or before the time or, as soon as practicable after, an APP entity collects personal information, it must take such steps (if any) as are reasonable in the circumstances:
  - a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or
  - b) to otherwise ensure that the individual is aware of any such matters.

(APP 5.1)



# Notification of collection of personal information

## » APP 5.2 *includes*:

- identity and contact details of the APP entity
- purposes of collecting the information
- main consequences (if any)
- disclosure to any other entity or person or overseas
- the relevant privacy policy
- details of access to or how to correct such information



# Tax File Number



[aitken.com.au](http://aitken.com.au)



[@aussie\\_lawyer](https://twitter.com/aussie_lawyer)



[/company/aitken-partners](https://www.linkedin.com/company/aitken-partners)

**aitken**  
partners

# File number recipient

- » A person who is (whether lawfully or unlawfully) in possession or control of a record that contains tax file number information shall be regarded, for the purposes of this Act, as a file number recipient (s11).
- » Where the record of the tax file number information is in the possession or under the control of a person...  
(s11(2))

# TFN - Interference with Privacy

An act or practice is an interference with the privacy of an individual if:

- (a) it is an act or practice of a file number recipient and the act or practice breaches a rule issued under section 17 in relation to tax file number information that relates to the individual; or
- (b) the act or practice involves an unauthorised requirement or request for disclosure of the tax file number of the individual.

(s 13(4))

# Rules relating to tax file number information

- » The Commissioner must, by legislative instrument, issue rules concerning the collection, storage, use and security of tax file number information (s17).
- » A file number recipient shall not do an act, or engage in a practice, that breaches a rule issued under section 17 (s18).

# TFN Rule

- » *Privacy (Tax File Number) Rule 2015* (TFN Rule) issued under s 17 of the Privacy Act
- » Regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN information
- » Only applies to individuals and not entities
- » Legally binding and breach is an interference with privacy under the Privacy Act

# Collection of TFN Information

- » The recipients must only collect a TFN from individuals and other TFN recipients for a purpose authorised by law, is not unreasonably intrusive, and necessary and relevant for the purpose under the relevant law.
- » When requesting an individual's TFN, the TFN recipients must take reasonable steps to ensure that the individuals are informed of:
  - o authorising law;
  - o purpose;
  - o right to, and consequences of declining.

(see r8)

# Other relevant rules

- » Use or disclose for authorised purpose
- » Take reasonable steps to:
  - protect from misuse, loss, and unauthorised....
  - ensure access is restricted
  - securely destroy or permanently de-identify where...

(see r10 & 11)



# TFN Rule - Staff Training

- » The recipients must take reasonable steps to ensure that all staff are ware of the need to protect individuals' privacy when handling TFN information and the rules of collection including: (r12)
  - circumstances where the TFN can be collected;
  - prohibitions on use and disclosure;
  - need to protect the individual's privacy' pursuant to the law; and
  - penalties or other sanctions that apply for a breach.



Ric Birkett

# Notifiable Data Breaches



[aitken.com.au](http://aitken.com.au)



[@aussie\\_lawyer](https://twitter.com/aussie_lawyer)



[/company/aitken-partners](https://www.linkedin.com/company/aitken-partners)

**aitken**  
partners

# What's it all about?

- » This is high level (there always exceptions to the rules)
- » Part IIIIC to the *Privacy Act 1988* deals with the Notifiable Data Breaches (NDB) scheme.
- » Came into effect on 22 February 2018.
- » Requires notification of Eligible Data Breaches (EDBs) to:
  - The Information Commissioner; and
  - Individuals affected by the EDB.
- » Optus (Sept 2022) and Medibank (Oct 2022) great examples of how it can happen and the consequences (PR nightmare and both under OAIC investigation)

# Why should I care?

- » Failure to comply constitutes an interference with the privacy of an individual and if considered “serious” or “repeated” may be an offence under Section 13G.
- » Penalties (increased in December 2022):
  - Individual – up to \$2.5m (was was \$444,000);
  - Body corporate – up to \$50m (was \$2.22m).
- » New powers for OAIC to investigate breaches but also pre-emptive powers to access ability to comply (with new infringement notice powers to enforce failures to provide information).

# Why should I care?

- » Now more than ever “privacy” is more than just a buzz word particularly as consequences of privacy breaches become more common. Optus and Medibank were very high profile and highlighted the risks (and became a political issue).
- » Now an area of real risk with broader exposure to claims by individuals affected by data breaches.
- » Risk of significant reputational damage flows from failures to protect the data of individuals, to rapidly and properly respond to breaches or to try to cover up the unauthorised access, disclosure or loss of personal information.

# What does the NDB apply to?

- » Unauthorised access to, disclosure of or loss of “personal information” (reminder):

*personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:*

- (a) whether the information or opinion is true or not; and*
- (b) whether the information or opinion is recorded in a material form or not.*

- » Does not apply to events that do not involve personal information. Consider whether the information the subject of the event is actually “personal information”.

# When is a data breach an Eligible Data Breach (EDB)? (Section 26WE)

When there is:

- » unauthorised access or disclosure of personal information (actual access or disclosure) or personal information is lost and unauthorised access or disclosure is likely to occur (likely access or disclosure); **and**
- » a reasonable person would conclude that the access, disclosure or loss would be likely to result in serious harm to the individual or individuals it relates to.

# When is a data breach an Eligible Data Breach (EDB)? (Section 26WE)

- » Unauthorised access or disclosure – e.g. hacked, an employee accesses the data who is not authorised or for a purpose that is not authorised, accidentally disclosed to the wrong person or a person who is not authorised to receive it (including by deception).
- » Lost – eg documents or devices containing personal information lost or left behind (public transport, restaurant, etc). Must still be likely that unauthorised access or disclosure will occur.



# Risk of serious harm (Section 26WG)

- » Not an EDB unless a reasonable person would conclude that it is likely to result in serious harm.
- » Reasonable person viewed from the point of view of the entity and not the individual whose information is involved.

# Risk of serious harm (Section 26WG)

- » OAIC suggests that the types of risks causing harm include:
  - identity theft
  - significant financial loss by the individual
  - threats to an individual's physical safety
  - loss of business or employment opportunities
  - humiliation, damage to reputation or relationships
  - workplace or social bullying or marginalisation
- » “Serious Harm” not defined. OAIC suggests that it may include “physical, psychological, emotional, financial, or reputational harm”.

# Risk of serious harm (Section 26WG)

- » Act requires that the following be considered in assessing whether a reasonable person would consider there is likely to be serious harm:
  - the kind or kinds of information
  - the sensitivity of the information
  - whether the information is protected by one or more security measures
  - if the information is protected by one or more security measures – the likelihood the security measures could be overcome
  - the persons, or the kinds of persons, who have obtained, or who could obtain, the information

# Risk of serious harm (Section 26WG)

- if a security technology or methodology was used in relation to the information and was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information (e.g. encrypted), the likelihood that the persons, or the kinds of persons, who:
  - have obtained, or who could obtain, the information; and
  - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates,have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology
  - the nature of the harm
  - any other relevant matters.

# Risk of serious harm (Section 26WG)

- » Volume of data may be relevant. The more data, the greater the risk that one or more individuals may suffer serious harm
- » AOIC resources provide its views on this matter and include other considerations and examples

# When is an Eligible Data Breach not an Eligible Data Breach? Remedial Action (Section 26WF)

- » If loss of personal information occurs and take action before unauthorised access or disclosure occurs and as a result there is no unauthorised access or disclosure - not an EDB.
- » If unauthorised access or disclosure of personal information occurs and take action before it results in serious harm to any individual and as a result of the action a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm - not an EDB.

# When is an Eligible Data Breach not an Eligible Data Breach? Remedial Action (Section 26WF)

- » If loss, and take action after unauthorised access or disclosure but before serious harm and reasonable person would conclude not likely to result in serious harm - not an EDB.
- » If action will only avoid harm to some individuals, still EDB but not required to notify those individuals who are unaffected.

# When is an Eligible Data Breach not an Eligible Data Breach? Remedial Action (Section 26WF)

- » Examples of remedial action:
  - Accidentally send personal information to a recipient. Contacts recipient and confirms that the information has not been distributed or misused and has been permanently deleted. Regards the recipient as reliable and trustworthy and confident that there is no risk of harm.
  - Leave phone on public transport:
    - Retrieve phone and confident data has not been accessed
    - Phone enables remote deletion of data which is done and consider that this is likely to prevent access or misuse.
- » Document all remedial actions carefully and have processes for sign off on actions



# What if there might have been a breach but I'm not sure? Investigate (Section 26WH)

» If:

- an entity is aware that there are reasonable grounds to **suspect** that there may have been an eligible data breach of the entity; and
- the entity is not aware that there are reasonable grounds to **believe** that the relevant circumstances amount to an eligible data breach of the entity.

The entity must carry out a reasonable and expeditious assessment and take all reasonable steps to complete the assessment within 30 days.

# What if I believe there has been an EDB? Notification to Commissioner (Section 26WK)

- » If aware that there are reasonable grounds to **believe** an EDB, must, as soon as practicable after becomes aware, prepare, and give to the Information Commissioner, a statement that sets out:
  - the identity and contact details of the entity; and
  - a description of the eligible data breach that the entity has reasonable grounds to believe has happened; and
  - the kind or kinds of information concerned; and
  - recommendations about the steps that individuals should take in response to the eligible data breach that the entity has reasonable grounds to believe has happened.

# What if I believe there has been an EDB? Notification to Individuals (Section 26WL)

- » If aware that there are reasonable grounds to **believe** an EDB has occurred, must, as soon as practicable after completing the statement to the Commissioner:
  - if practicable, take reasonable steps to notify the content of the statement to each individual to whom the relevant information relates;

OR

# What if I believe there has been an EDB? Notification to Individuals (Section 26WL)

- if practicable, take reasonable steps to notify the content of the statement to each of the individuals who are at risk from the EDB;

OR

- only if not practicable to do either of the above, publish the statement on the entity's website and take reasonable steps to publicise the EDB.

# Overseas recipient (Section 26WC)

- » If you provide personal information to an overseas recipient, the personal information is deemed to be held by the disclosing entity (you).
- » If the overseas recipient is the subject of an EDB, the EDB is deemed to be an EDB of the disclosing entity (you).
- » Some exceptions (see APP 8).

# Other actions by Commissioner.

- » Declaration that notification requirements do not apply or allowing specified time for compliance (i.e. beyond “as soon as practicable”) (Section 26WQ)
  - Commissioner must have regard to:
    - Public interest
    - Advice from enforcement bodies and Defence (and others)
    - Other matters Commissioner considers relevant
  - Notification requirements suspended while Commissioner considers application for declaration.
- » Direct an entity to comply with the notification requirements (Section 26WR)
  - if the entity has not done so itself.

# Some stats

- » Between 1 April 2018 (two months after commenced) and 30 June 2022:
  - Total NDBs reported: 4,109
- » Of these:
  - Under 100 people affected: 2,753 (67%)
  - Health sector has topped this list of number of reports in every reporting period and accounted for 675 of the total reports 16.5%.
- » Majority have involved malicious attacks (roughly two thirds) but also a large portion are due to human error (roughly one third). System failure runs at around 4-5%.

# What else might be coming?

- 16 Feb 2023 – A-G released Privacy Act Review Report
- 116 proposals for change, many of which will impact EDB scheme
- Reduction of the period to investigate and report **suspected** breach from 30 days to 72 hours.
- Broader definitions of personal information
- Privacy impact assessments for high privacy risk activities
- Individual rights of action (statutory tort of privacy) where intentional or reckless breaches
- Further enhanced penalty and enforcement provisions...  
and much, much more.



# What should I do?

- » If you don't need it, don't collect it
- » If you don't need it any more, get rid of it
- » Have strong IT security systems – anti- malware, multi-factor identification, up to date firewall, etc
- » Think about how data is stored (can it be deidentified / encrypted)
- » Have clear policies and procedures relating to employee use and holding of data including security protections – encryption, device passwords, remote delete options
- » Choose your suppliers and contractors carefully, particularly IT providers (including cloud). Look for security credentials like ISO 27001 certification.

# What should I do?

- » Know where your data is and who has access to it – make sure they are compliant (and have obligations to be)
- » Have a Data Breach Response Plan – minimise risk of harm and act quickly so that remedial action is effective. See OAIC – “Data Breach and Response”
- » Comply if there is an EDB. Not just a legal issue but public criticism will follow for those who hesitate
- » Consider PR crisis response plan if this occurs.



# Privacy for Health Providers



[aitken.com.au](http://aitken.com.au)



[@aussie\\_lawyer](https://twitter.com/aussie_lawyer)



[/company/aitken-partners](https://www.linkedin.com/company/aitken-partners)

**aitken**  
partners

# Privacy Act 1988

- » 'Health Service' is captured regardless of the size of the business (\$3m 'small business rule' does not apply)
- » 'Health Service' is an activity performed:
  - To assess, maintain, improve or manage an individual's health
  - To diagnose or treat illness, disability or injury
  - To record an individual's health for these purposes
  - In dispensing medications by a pharmacist
- » E.g. doctors, allied health professionals, aged and disability care providers, hospitals, clinics and practices

# Health Records Act 2001 (Vic)

- » Victorian legislation
- » Applies in addition to the Privacy Act requirements but other inconsistent legislative provision take priority over HR Act
- » Applies to 'health service providers' and others who collect, hold or use 'health information'
- » 'Health service providers' – similar definition to 'health service' under Privacy Act but expressly includes disability service, palliative care service and aged care service
- » Applies to 'health information' – similar to Privacy Act definition

# Health Records Act 2001 (Vic)

## » Sets out 11 Health Privacy Principles (HPPs)

- HPP1 – Collection
- HPP2 – Use and disclosure
- HPP3 – Data quality
- HPP4 – Data Security and data retention
- HPP5 – Openness
- HPP6 – Access and correction
- HPP7 - Identifiers

# Health Records Act 2001 (Vic)

- HPP8 – Anonymity
  - HPP9 – Transborder data flows
  - HPP10 – Transfer or closure of practice/health provider
  - HPP11 – Making information available to other health practitioner
- » Many mirrored terms applying in Privacy Act
- » Some differences – e.g. applies to health information about deceased person (unlike Privacy Act)
- » No specific data breach notification scheme

# My Health Records Act 2012 (Cth)

- » Digital system for recording and sharing centralised health records
- » Act limits when and how health information included in a My Health Record can be collected, used and disclosed.
- » Unauthorised collection, use or disclosure of My Health Record information is breach of the My Health Records Act and recognised as an interference with privacy.
- » Includes a mandatory data breach notification scheme similar to that applying under the Privacy Act (and the Privacy Act exempts compliance with the NDB scheme if reported under this scheme)



# Aged Care Act 1997 (Cth)

- » Applies to all aged care approved providers (including home care)
- » General obligation under Act to comply with all laws
- » Specific obligations in relation to protection of 'personal information' (Division 62) and this compliance is expressly noted as a responsibility of an 'approved provider' (Division 56)
- » Offences exist under the Act for improper disclosure of personal information

# Aged Care Act 2001 (Cth)

- » User Rights Principles include a care recipient's right to *'personal privacy and to have my personal information protected'*
- » Resident Agreements must include *'a guarantee that all reasonable steps will be taken to protect the confidentiality, so far as legally permissible, of information provided by the care recipient'*
- » Includes document retention requirements



# Employee Records Exemption Privacy & Employment Law



[aitken.com.au](http://aitken.com.au)



[@aussie\\_lawyer](https://twitter.com/aussie_lawyer)



[/company/aitken-partners](https://www.linkedin.com/company/aitken-partners)

**aitken**  
partners

# OVERVIEW

- » Interaction between privacy and employment law in relation to an employee's 'personal information'
- » 'Employee records exemption', what it means for private sector employers
- » When will the APPs apply to private sector employers
- » Best practice to adopt by employers
- » Proposed reforms – Privacy Act Review Report

# Employee Record Exemption

- » Certain employers are exempt from complying with the Privacy Act if the Employee Record Exemption applies
- » An organisation that is or was an employer of an individual, is exempt from the operation of the Privacy Act where its act or practice is related directly to the employment relationship between the organisation and the individual, and an employee record held by the organisation (s 7B(3))
- » ‘Employee Record’ - “a record of personal information relating to the employment of the employee”

# Employee Record Exemption

- » Applies to private sector employers
- » Applies to employees (not information about independent contractors or unsuccessful job applicants)
- » Applies to information which is held by an employer (the information must exist)
- » Applies where the handling of the information relates directly to the employment relationship (there must be an “*absolute, exact or precise connection*” between the use or disclosure of the information and the employment relationship)

# Scenarios

- » Don't assume all information held is an employee record
- » Whilst information will likely relate to an employee, it may not directly relate to the employee's work activities
- » Information marketing goods or services (discount vouchers, insurance or health services )
- » Emails from third parties
- » Medical information about an illness unrelate to the job
- » Monitoring activities beyond genuine business needs

# Best Practice Measures

- » Develop a privacy policy outlining how an employee's personal information will be collected, used or disclosed
- » Collect personal information needed for legitimate work purposes. Keep employee records secure and updated
- » Cover expectations about the use of email, internet and social media, and any monitoring by employers
- » Provide training to those entrusted with the handling of personal information
- » Share the policy with workers and encourage discussion



# Privacy Act Review Report

- » Proposals are not law but likely to be in 2023
- » Employee Records Exemption to be retained but narrowed
- » Private sector employers to notify the regulator of any data breach involving an employee's personal information likely to result in serious harm
- » Private sector employers can't relax thinking the APPs don't apply to them, assume they do and incorporate best practices



# Summar Altaee Privacy Act Review



[aitken.com.au](http://aitken.com.au)



[@aussie\\_lawyer](https://twitter.com/aussie_lawyer)



[/company/aitken-partners](https://www.linkedin.com/company/aitken-partners)

**aitken**  
partners

# Proposed reforms...

- » What information should be protected and who should protect it?
- » What privacy protections should apply?
- » How should breaches of privacy be enforced?

A person in a suit is holding a document with a padlock on it. The background is a dark blue grid with binary code (0s and 1s) overlaid. There are yellow and black diagonal stripes in the corners.

# Current Commissioner Initiated Investigations (CII)

# Ongoing CI

Investigation focus	Date opened
Medlab	5 December 2022
Medibank	1 December 2022
Optus	11 October 2022
Bunnings and Kmart	12 July 2022
Optus	2 August 2021



# Recent Decisions



[aitken.com.au](http://aitken.com.au)



[@aussie\\_lawyer](https://twitter.com/aussie_lawyer)



[/company/aitken-partners](https://www.linkedin.com/company/aitken-partners)

**aitken**  
partners

- » *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021)*
- » *'WR' and Telstra Corporation Limited (Privacy) [2021] AICmr 5 (11 February 2021)*
- » *Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. (Privacy) [2021] AICmr 34 (30 June 2021)*

# PRIVACY 2023



**Julie Maxfield**

Principal

Aitken Partners

(03) 8600 6045

[jmaxfield@aitken.com.au](mailto:jmaxfield@aitken.com.au)



**Ric Birkett**

Principal Lawyer

Aitken Partners

(03) 8600 6005

[rbirkett@aitken.com.au](mailto:rbirkett@aitken.com.au)



**Bhrig Chauhan**

Principal Lawyer

Aitken Partners

(03) 8600 6019

[bchauhan@aitken.com.au](mailto:bchauhan@aitken.com.au)



**Summar Altaee**

Associate

Aitken Partners

(03) 8600 6069

[saltaee@aitken.com.au](mailto:saltaee@aitken.com.au)