ADEA Privacy Policy

July 2019



ADEA Privacy Policy

Version	Date	Name(s)	Notes
1	2016	ADEA	Created and approved
2	2018	Louise Gilmour	Revised
3	12 March 2018	Joanne Ramadge	Approved
4	8 July 2019	Vy Le	Revised
Final	23 August 2019	ADEA Board	Approved
Next review	February 2021		

File path: S:\Operational\Governance-Strategic\Final Approved Policy\Board Approved

Uncontrolled when printed Page 2 of 8

Acknowledgements

About ADEA

The Australian Diabetes Educators Association (ADEA) is the peak national organisation for multidisciplinary health professionals who are committed to the provision and excellence of quality, evidence-based diabetes education, care and management with over 2,300 members working in all sectors and across all locations.

ADEA aims to improve the health and wellbeing of people with diabetes by:

- 1. Assessing diabetes educators based on their qualifications, skills, knowledge and experience through the credentialling program
- 2. Supporting multidiscipline health professionals through its various programs, including mentoring, education and research
- 3. Developing and updating relevant policies, standards of practice and clinical guidelines

For more information, visit our website at www.adea.com.au.

Uncontrolled when printed Page 3 of 8

Table of Contents

ADEA Privacy Policy	2
Acknowledgements	3
About ADEA	3
Overview	5
Collecting information	5
Disclosing information	5
Unauthorised disclosure or access	6
Opt- out	6
Access to personal information	6
Security	6
Data Quality	6
Notifiable Data Breaches	Error! Bookmark not defined.
Privacy Inquiries	8
Availability and review of Policy	8

Overview

ADEA is committed to complying with the <u>Privacy Act 1988</u> and the <u>Australian Privacy Principles</u> <u>2014</u> and the privacy provisions of all applicable legislation. Updated Privacy laws commenced on 12 March 2014 that introduced the new Australian Privacy Principles ('APPs'). The APPS set out the way organisations and government agencies such as the Australian Diabetes Educators' Association can collect, use, disclose, secure and provide access to personal information.

This privacy policy covers all personal information we hold, that is, information, or an opinion about an individual, whose identity is apparent, or can be reasonably ascertained, from that information or opinion. This includes information we have collected from people through our office, over the phone and over the internet.

Collecting information

When we collect personal information from an individual, we will ensure that we do so in a fair manner and that we let the individual know where and how to contact our organisation. We will only collect information that is reasonably necessary for our functions or activities.

We will advise individuals or the purpose for which their personal information is collected.

If we collect sensitive information (as defined under the Act), we will treat it with the utmost security and confidentiality. We will ensure that it is not collected for any purposes, other than those for which we have obtained the individual's consent, unless the law requires otherwise, or other exceptional circumstances prevail as described under the Act.

Where an individual chooses not to provide requested information, we will advise that individual of what consequences this non-disclosure may have. For example, withholding certain information may limit our ability to provide relevant offers or services to individuals.

ADEA will take reasonable steps to ensure data is accurate, up-to-date and complete.

Using and disclosing information

We will only use and disclose personal information in accordance with the Privacy Act. This means that personal information may be used or disclosed:

- For the purposes for which we have advised that we are collecting it, and for related purposes that the individual would reasonably expect,
- Where we have the consent of the individual to do so,
- As required by law, or
- Under other circumstances where permitted under the Act.

In the course of our business activities, we may need to disclose some of your personal information to relevant staff.

ADEA does not disclose personal information to overseas recipients in any circumstances.

Uncontrolled when printed Page 5 of 8

Unauthorised disclosure or access

As ADEA is committed to protecting the privacy of individuals, we will view unauthorised disclosure of, or access to, personal information by our employees or contractors, as a serious breach of this policy. Appropriate action (which may include disciplinary or legal action) will be taken in such cases.

Opt- out

We will always provide individuals with a nil-cost way of contacting us to register a request to "opt-out" from receiving any product offers and direct marketing communications.

Access to personal information

ADEA members can access their personal information via the membership dashboard.

Individuals will be able to access their personal information upon request. However, ADEA may occasionally need to deny access to information in accordance with the exemptions contained in the Act.

Security

Our goal is to protect the personal information collected by ADEA and its associations. Personal information will be managed confidentially and securely and destroyed appropriately when no longer required. We will monitor and implement appropriate technical advances or management processes, to safeguard personal information.

Data Quality

We will take all reasonable steps to ensure that the data we collect, use or disclose is accurate, complete and up to date, and has been obtained directly from individuals or other reputable sources.

ADEA members are required to review and update their details regularly to keep them accurate, upto-date and complete. Non-member individuals will also able to have their information corrected if their details have become out-of-date.

Data Breach Notification Scheme

The Privacy Act establishes a mandatory Data Breach Notification Scheme (DBN Scheme) which requires ADEA to notify particular individuals and the Office of the Australian Information Commissioner about 'eligible data breaches'.

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information that an entity holds. A data breach is eligible if it is likely to result in serious farm to any of the individuals to whom the personal or sensitive information relates. ADEA will make an objective assessment of whether a data breach is likely to result in serious harm and take remedial action according to its data breach response plan.

Uncontrolled when printed Page 6 of 8

Data breach response plan

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- Initiate: plan the assessment and assign a team or person
- Investigate: gather relevant information about the incident to determine what has
 occurred
- Evaluate: make an evidence-based decision about whether serious harm is likely. OAIC
 recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO Is serious harm still likely?

YES

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- Option 1: Notify all individuals
- . Option 2: Notify only those individuals at risk of serious harm

If neither of these options are practicable:

• **Option 3:** publish the statement on the entity's website and publicise it Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- · Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- · police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- · professional bodies
- · your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Refer to the ADEA Data management and response plan for further details.

Uncontrolled when printed Page 7 of 8

Privacy Inquiries

Privacy related inquiries or concerns can be directed to the ADEA Privacy Officer on 02 6173 1000.

Availability and review of policy

We will make our privacy policy available upon request and will provide a link to this policy from our website.

This policy will be reviewed from time to time and any amendments will be incorporated into the updated policy.

Uncontrolled when printed Page 8 of 8