Indigenous Allied Health Australia
PO Box 323 Deakin West ACT 2600
Phone: +61 2 6285 1010
Fax: +61 2 6260 5581
www.iaha.com.au

Policy Title: Privacy and Confidentiality

1. POLICY STATEMENT

Indigenous Allied Health Australia (IAHA) Ltd. understands that privacy and confidentiality is important to our members, employees, students, representatives, and Board Directors and subsidiary company IAHA NT Workforce Development (IAHA NT WD) Ltd.

Unless otherwise required by law, confidential information will be treated as such, and personal information will be utilised only for the purpose intended. Such personal information will not be disclosed to any other organisations or to any other individuals without express permission from the individual to whom the details relate, save where the law requires such information to be divulged.

While this policy outlines IAHA's privacy and confidentiality obligations, IAHA are committed to best and ethical practices with respect to Indigenous Data Sovereignty and related considerations.

2. PURPOSE

This policy records the principles IAHA adopts regarding personal information held by IAHA in respect to its members, employees, representatives, Board Directors, students, or subsidiary company IAHA NT WD. These principles are determined by IAHA's legislative requirements under the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* and the *Information Privacy Act 2014 (ACT) and Information Privacy Act 2000 (Vic) and NT Information Act 2002*.

This document:

2.1. Is binding on all IAHA and IAHA NT WD members, representatives, Board Directors, students, and employees and any other individuals who have access to personal information held by IAHA and/or IAHA NT WD.

2.2. Establishes the IAHA policy and procedures for addressing privacy and confidentiality issues in implementing IAHA business.

3. DEFINITIONS

3.1. **Personal information:** Personal information is very broad and generally refers to any information or opinion about a particular individual or a person who could be easily identified. Even if this information or opinion is untrue or inaccurate, it may still be considered personal information under the law. The information also does not need to be in written form. Some examples of personal information include an individual's:

a) name
b) address
c) phone number
d) date of birth
e) signature
f) email
g) bank account details
h) racial origin
i) education
j) religion

3.2. **Sensitive Information:** Sensitive information is a type of personal information but unlike some personal information - sensitive information may result in discrimination or harm if it is mishandled. Sensitive information may include, but is not limited to, any information or opinion about an individual's race or ethnic origin, political opinions or membership of a political organisation, religious beliefs and affiliations, philosophical beliefs, membership of a professional association or trade union, sexual preferences and orientation, criminal record, health information, genetic information, biometric information.

3.3. **User**: means an individual either private or part of an organisation that accesses the IAHA or IAHA NT WD websites.

3.4. **Australian Privacy Principles (APP)**: The Australian Privacy Principles, provided at Attachment B, are the cornerstone of the privacy protection framework in the *Privacy Act 2000*.

3.5. **APP Entity**: An APP entity is, generally speaking: an agency (which largely refers to a federal government entity and/or office holder) or an organisation (which includes an individual, body corporate, partnership, unincorporated association, or trust) with obligations under the Privacy Act.

3.6. **Enforcement body or Agency**: Includes the Australian Federal Police, Customs, Integrity Commission, and any government body of the Commonwealth or of a State or Territory that are privacy and law enforced agencies for the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law.

3.7. **Board or Board Directors:** Members of the IAHA and/or IAHA NT WD Board of Directors.

3.8. **Employee:** Staff member of IAHA, including trainees.

3.9. **Students:** Students enrolled in the National Aboriginal and Torres Strait Islander Health Academy or other IAHA activities or programs.

3.10. **Representative:** an appointed or chosen person delegated and approved by IAHA to speak, act, represent, attend, or observe on behalf of IAHA, at various forums.

3.11. **Member:** Members of IAHA.

4. POLICY / PROCEDURES

4.1. Collection

Where APPs are mentioned, reference can be made to the Summary of Australian Privacy Principles or detailed information for the Australian Privacy Principles, both of which can be found here https://www.oaic.gov.au/privacy/australian-privacy-principles.

4.1.1 Personal Information other than Sensitive Information.

IAHA will not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of IAHA's functions or activities.

IAHA will only collect personal information from those individuals who are members of IAHA, members of the Board of IAHA, employees, students, or representatives of IAHA and/or IAHA NT WD, where required.

4.1.2 Sensitive Information.

IAHA will not collect sensitive information about an individual unless:

- the individual consents to the collection of the information and;
- the information is reasonably necessary for one or more of IAHA's functions or activities; or
- subclause 4.1.3 below, where it applies in relation to the information.

4.1.3 Collecting sensitive information where a permitted general situation exists

This subclause applies in relation to sensitive information about an individual where:

- the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or
- a permitted general situation exists in relation to the collection of the information by IAHA; or
- a permitted health situation exists in relation to the collection of the information by IAHA; or where Government directives request this i.e. vaccination records for pandemics, or
- the collection of the information is reasonably necessary for, or directly related to, one or more of IAHA's functions, events, or activities; or
- the information relates to the business activities of IAHA and/or IAHA NT WD i.e. police checks, working with vulnerable people or children checks; or
- the information relates solely to the members of IAHA, or to individuals who have regular contact with IAHA and IAHA NT WD in connection with its activities.

4.1.4 Collection by lawful and fair means.

IAHA will collect personal or sensitive information only by lawful and fair means and will only collect personal or sensitive information from the individual concerned, unless:

- there is a lessening or preventing serious threat to life, health, or safety and its unreasonable or impracticable to obtain the individuals consent to the collection, or
- the individual consents to the collection of the information from someone other than themselves; or
- IAHA is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual.

4.1.5 Dealing with unsolicited information.

IAHA must decide within a reasonable period when receiving unsolicited personal or sensitive information whether or not IAHA could have collected the information under the *Australian Privacy Principle 3 - Collection of Solicited Information* (APP3), and whether:

- IAHA may use or disclose the personal or sensitive information for the purposes of making the determination under the above point.
- If it is determined that IAHA could not have collected the personal or sensitive information, and the information is not contained in a Commonwealth record, IAHA must destroy or de-identify or securely file the information as soon as practicable but only if it is lawful and reasonable to do so.
- If IAHA could have collected the information under APP3 or the information is contained in a Commonwealth record, or IAHA is not required to destroy or de-identify the information under *Australian Privacy Principle 4.3* because it would be unlawful or unreasonable to do so - IAHA must deal with it in accordance with *Australian Privacy Principles 5 to 13 (APP5-13)*.

- If the above does not apply in relation to the personal or sensitive information, notification of collection policy applies in relation to the information as if IAHA had collected the information under *Australian Privacy Principle 3 - Collection of Solicited Information*.

4.1.6 Notification of the collection of personal information.

When IAHA collects personal or sensitive information about an individual, it will take reasonable steps to either notify an individual of certain matters or to ensure the individual is aware of those matters before or at the time it collects personal or sensitive information. If such notification is not practicable or reasonable, steps will be taken as soon as practicable after collection.

The matters referred to in subclause 4.1.6.1 as are reasonable in the circumstances.

4.1.6.1 Matters about which an individual must be notified or made aware

The matters for the purposes of subclause 4.1.6 are as follows:

- The identity and contact details of IAHA and where relevant IAHA NT WD.
- if:
  - IAHA collects the personal or sensitive information from someone other than the individual; or
  - the individual may not be aware that IAHA has collected the personal or sensitive information;
  - the fact that IAHA so collects or has collected the information and the circumstances of that collection.
- The matter set out in APP5.2(c) is the fact (if applicable) that collection of the personal or sensitive information is required or authorised by or under an Australian law or a court/tribunal order. The phrase 'required or authorised (by or under Australian law, or court/tribunal order', is discussed in Chapter B of the APP.
- The facts and circumstances of collection - purposes for which IAHA collects the personal or sensitive information.
- The consequences (if any) for the individual if all or some of the personal or sensitive information is not collected by IAHA.
- Any other Australian Privacy Principles (APP) entity, body or person, or the types of any other APP entities, bodies, or persons, to which IAHA usually discloses personal or sensitive information of the kind collected by IAHA.
- That *IAHA's Privacy and Confidentiality Policy* contains information about how the individual may access the personal or sensitive information about the individual that is held by IAHA and seek the correction of such information.
- That *IAHA's Privacy and Confidentiality Policy* contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds IAHA, and how IAHA will deal with such a complaint.
- Whether IAHA is likely to provide cross-border disclosures of the personal or sensitive information i.e. to overseas recipients and if so,
- the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

4.2. Use and Disclosure

Personal or sensitive information IAHA holds about an individual that was collected for a particular purpose (the primary purpose), must not be used, or disclosed for another purpose (the secondary purpose) unless:

- the individual has consented to the use or disclosure of the information; or
- subclauses 4.2.1 or 4.2.2 applies in relation to the use or disclosure of the information.

4.2.1 Using or disclosing personal or sensitive information related to the primary purpose of collection and the individual's reasonable expectations of IAHA to do so

IAHA is permitted to use or disclose personal or sensitive information about an individual if the individual would reasonably expect IAHA to use or disclose the personal or sensitive information for the secondary purpose and the secondary purpose is:

- if the information is sensitive information — directly related to the primary purpose of collection; or
- if the information is not sensitive information — related to the primary purpose of collection; or
- the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or
- a permitted general situation exists in relation to the use or disclosure of the information by IAHA; or
- IAHA reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

4.2.2 De-identifying certain information before disclosure

IAHA must take such steps as are reasonable in the circumstances to ensure that certain personal or sensitive information is de-identified before IAHA discloses it.

4.3. Data quality

IAHA must take such steps (if any) as are reasonable in the circumstances to ensure that the personal or sensitive information that IAHA collects, uses, or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete, and relevant.

4.4. Data security

If IAHA holds personal or sensitive information, IAHA must take such steps as are reasonable in the circumstances to protect the information from misuse, interference, and loss, as well as unauthorised access, modification, or disclosure.

Personal or sensitive information about an individual held by IAHA will be stored in a safe and secured facility and will only be available as is reasonably necessary in order for IAHA to adequately conduct business.

IAHA will take such steps as are reasonable in the circumstances to destroy or de-identify or securely file personal or sensitive information in any of the following situations:

- where member information is no longer relevant, or
- IAHA no longer needs the information for any purpose for which the information may be used or disclosed by IAHA under this Schedule; or
- the information is not contained in a Commonwealth record; or
- IAHA is not required by or under an Australian law, or a court/tribunal order, to retain the information.

IAHA will also strive to preserve the integrity of the personal or sensitive data stored, either physically or electronically, by updating this data. Additionally, electronic information is

protected by way of firewall against electronic threat.

4.5. Openness

4.5.1 Compliance

IAHA is committed to manage personal or sensitive information in an open and transparent way. To achieve this, IAHA must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to IAHA's functions or activities that:

- ensure that IAHA complies with the Australian Privacy Principles and a registered APP code (if any) that binds IAHA; and
- enable IAHA to deal with inquiries or complaints from individuals about IAHA's compliance with the Australian Privacy Principles or such a code.

IAHA has a clearly expressed an up to date policy about the management of personal or sensitive information which contains:

- the kinds of information that IAHA collects and holds;
- how IAHA collects and holds information;
- the purposes for which IAHA collects, holds, uses, and discloses information;
- how an individual may access information about the individual that is held by IAHA and seek the correction of such information;
- how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds IAHA, and how IAHA will deal with such a complaint;
- whether IAHA is likely to disclose personal or sensitive information to overseas recipients and
- the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

4.5.2 Availability

IAHA takes such steps as are reasonable in the circumstances to make its *Privacy and Confidentiality Policy* available free of charge and in such form as is appropriate. Noting that the policy is also available on IAHA's website.

If a person or body requests a copy of *IAHA's Privacy and Confidentiality Policy* in a particular form, IAHA will take such steps as are reasonable in the circumstances, to give the person or body a copy in that form.

IAHA will ensure continued compliance with this policy by way of annual review by the IAHA Board. Compliance with this policy is mandatory for all who are bound by it.

4.6. Access and correction

Access to any personal or sensitive information IAHA holds about an individual must, on request by the individual, be given.

4.6.1 Exception to access

IAHA is not required to give the individual access to the personal or sensitive information to the extent that:

- IAHA reasonably believes that giving access would pose a serious threat to the life, health, or safety of any individual, or to public health or public safety; or
- giving access would have an unreasonable impact on the privacy of other individuals; or

- the request for access is frivolous or vexatious; or
- the information relates to existing or anticipated legal proceedings between IAHA and the individual, and would not be accessible by the process of discovery in those proceedings; or
- giving access would reveal the intentions of IAHA in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- giving access would be unlawful; or
- denying access is required or authorised by or under an Australian law or a court/tribunal order; or
- IAHA has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to IAHA's functions or activities has been, or is being or may be engaged in and giving access would be likely to prejudice taking the appropriate action in relation to the matter; or
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; ~~or~~ and
- giving access would reveal evaluative information generated within IAHA in connection with a commercially sensitive decision-making process.

IAHA must:
- respond to the request for access to the personal or sensitive information within a reasonable period after the request is made; and
- give access to the personal or sensitive information in the manner requested by the individual, if it is reasonable and practicable to do so.

4.6.2 Other Means of Access

If IAHA refuses:
- to give access to the personal or sensitive information because of subclause 4.6.1; or
- to give access in the manner requested by the individual;

IAHA must:
- take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of IAHA and the individual. This should be done within 30 calendar days where practicable, and
- Without limiting subclause 4.6.1, access to the personal or sensitive information may be given through the use of a mutually agreed intermediary.

4.6.2.1 Access charges

Under APP12 if the APP entity is an organisation, such as IAHA – we cannot charge the individual for the making of the request or for giving access to personal or sensitive information.

4.6.3 Refusal to Give Access

If IAHA refuses to give access to the personal or sensitive information because of subclause 4.6.1, or to give access in the manner requested by the individual, IAHA must give the individual a written notice that sets out:
- the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and
- the mechanisms available to complain about the refusal; and
- any other matter prescribed by the regulations.

If IAHA refuses to give access to the personal or sensitive information because doing so would reveal evaluative information generated in connection with a commercially sensitive decision-making process – the reasons for the refusal may include an explanation for the commercially sensitive decision.

4.6.4 Correction

IAHA must take such steps (if any) as are reasonable in the circumstances to correct personal or sensitive information to ensure the purpose for which the information ~~it~~ is held, that the information is accurate, up to date, complete, relevant, and not misleading. Correction will apply when:

- IAHA is satisfied that, having regard to a purpose for which the personal or sensitive information is held, the information is inaccurate, out of date, incomplete, irrelevant, or misleading; or
- the individual requests IAHA to correct their information.

4.6.4.1 Notification of correction to third parties

Is required if

- IAHA corrects personal or sensitive information about an individual that IAHA previously disclosed to another APP entity; and
- If the individual requests IAHA to notify the other APP entity of the correction.

IAHA must take such steps (if any) as are reasonable in the circumstances to provide correction notification unless it is impracticable or unlawful to do so.

4.6.4.2 Refusal to correct information

If IAHA refuses to correct the personal or sensitive information as requested by the individual, IAHA must give the individual a written notice that sets out:

- the reasons for the refusal except to the extent that it would be unreasonable to do so; and
- the mechanisms available to complain about the refusal; and
- any other matter prescribed by the regulations.

4.6.4.3 Request to associate a statement

Is required if:

- IAHA refuses to correct the personal or sensitive information as requested by the individual; and
- the individual requests IAHA to associate with the information a statement that informs the information is inaccurate, out-of-date, incomplete, irrelevant, or misleading; then

IAHA must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

4.6.6.5 Dealing with requests

If a request is made for correction (subclause 4.6.4), or to associate a statement (subclause 4.6.4.3), IAHA must:

- respond to the request within a reasonable period after the request is made,

- must not charge the individual for the making of the request, for correcting the personal or sensitive information or for associating the statement with the personal information (as the case may be).

4.7. Identifiers

Members, Board Directors, students, and employees of IAHA shall not be identified by any identifier save that for which has been created by IAHA in order to identify members, Board Directors, students, and employees unless such identification is required in order to adequately carry out the services offered by IAHA.

4.8. Anonymity

Under APP2, wherever it is lawful and practicable, individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with IAHA in relation to a particular matter.

However, anonymity will not be an option for an individual, in relation to that matter if:

- IAHA is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or,
- it is impracticable and unreasonable for IAHA to deal with individuals who have not identified themselves or who have used a pseudonym.

4.9. Trans Border data flows

Before IAHA discloses personal or sensitive information about an individual to an overseas recipient/person that is:

- not in Australia or an external Territory;
- not the entity (IAHA) disclosing the personal or sensitive information, and
- not the individual to whom the personal information relates;

IAHA must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the *Australian Privacy Principles* in relation to the information at APP8.1.

IAHA will not disseminate or disclose personal or sensitive information about members, students, or employees to other State or Territory associated organisations.

4.10. Web use

4.10.1 IAHA and/or IAHA NT WD will collect and maintain in the database, certain personally identifiable information from members, students, or employees only when it is provided on a voluntary basis, for example, when making an enquiry.

4.10.2 Email addresses will be used only for the purpose for which they have been provided and will not be added to mailing lists or used for any other purpose without specific consent being given.

4.10.3 IAHA and/or IAHA NT WD will not share any information about website users with third parties except as provided by civil privacy legislation.

4.10.4 The IAHA and/or IAHA NT WD website does not provide facilities for secure transmission of information across the internet.

4.10.5 Internet Service Providers maintain records and log information about website visitors, including but not limited to:

a) user server addresses;
b) user top level domain names (i.e. .com, .*gov*, .au, .uk, etc.);
c) date and time of visit to the site;
d) pages accessed and documents downloaded;
e) previous site visited;
f) type of browser utilised to access the website and
g) any other information as is reasonably understood as being usual practice for Internet Service Providers to collect.

4.10.6 By using the IAHA and/or IAHA NT WD website, users consent to the *IAHA Privacy and Confidentiality Policy*.

4.10.7 Any changes to the *IAHA and/or IAHA NT WD Privacy and Confidentiality Policy* will be updated on the IAHA and IAHA NT WD website.

4.10.8 Users may consult the IAHA Privacy and Confidentiality Policy at any time in order to obtain details of the information collected, how it is used and the circumstances under which any of this information is disclosed, if at all.

4.10.9 Users may contact the IAHA CEO with any queries at admin@iaha.com.au

4.10.10 All information contained on the IAHA and/or IAHA NT WD website is Copyright ©Indigenous Allied Health Australia Ltd and/or ©IAHA NT Workforce Development Ltd.

4.10.11 All information contained on the IAHA and/or IAHA NT WD website is for the purposes of reference by interested visitors.

4.10.12 Information may be cited only with prior written permission and proper attribution.

4.10.13 Any queries regarding the use of material and information contained within the IAHA and/or IAHA NT WD website should be directed to the IAHA Communications team at comms@iaha.com.au

4.10.14 IAHA and/or IAHA NT WD accepts no responsibility for the content on external sites. External links are presented without warranty, express or implied. The descriptions of sites in these pages have been taken from the pages themselves and do not express the opinions of IAHA or IAHA NT WD.

4.11. Complaints

Any complaints can be directed to the IAHA CEO at admin@iaha.com.au in line with the IAHA Complaints Handling Policy.

4.12 Data Breach

In accordance with the *Privacy Amendment (Notifiable Data Breaches) Bill 2016,* IAHA in years when it's annual turnover exceeds $3million, must notify of eligible data breaches to the Office of the Australian Information Commissioner (OAIC) and affected individuals as soon as practicable after the applicable entity becomes aware that "there are reasonable grounds to believe that there has been an eligible data breach of the entity" (section 26WK of the Bill)

IAHA will refer to the legislation with regards to determining an eligible breach and act accordingly. Refer to Appendix 1 for flow chart re definitions of an 'eligible breach'.

5. ACKNOWLEDGEMENTS / REFERENCES

Australian Privacy Principles and
The Australian Government Office of the Australian Information Commission (OAIC)
IAHA Records and Information Management and Security Policy
IAHA Complaints Handling Policy
IAHA Code of Conduct Policy
IAHA Anti-Racism and Anti-Discrimination Policy
IAHA Indigenous Cultural and Intellectual Property Policy
IAHA Risk Management Policy
IAHA Social Media Policy
Representing IAHA Policy
IAHA Delegations Policy
IAHA Communications Policy
AIATSIS Code of Ethics for Aboriginal & Torres Strait Islander Research
https://aiatsis.gov.au/sites/default/files/2020-10/aiatsis-code-ethics.pdf

6. RELATED LEGISLATIONS

Privacy Act 1988 (Cth)
Privacy Amendment (Enhancing Privacy Protection Act 2012)
Health records Act 2001 (Vic)
Information Privacy Act 2014 (ACT)
Charter of Human Rights and Responsibilities Act 2006 (Vic)
Information Privacy Act 2000 (Vic)
NT Information Act 2002

7. DEVELOPED BY:

Effective Date:	14 April 2014
Reworked/redeveloped:	31 January 2023
Re-endorsed by the Board on:	2 March 2023
Review Date:	31 January 2024

Signed by the Chief Executive Officer: Date: 2 March 2023

Signed by the Chairperson: Date: 2 March 2023

Appendix 1
Mandatory Data Breach Notification Regime