Alicaring Pty Ltd
ABN:24 645 359 306
Phone: 07 3171 9713
Email: info@alicaring.com.au

PRIVACY AND CONFIDENTIALITY

Policy Statement

Alicaring Community accepts and abides by the National Privacy Principles to protect personal information set out in the Privacy Act 1988 (Cth) and amended by the Information Privacy Act 2009 (QLD) and other privacy laws. In so doing, all personal information collected by the organisation will be carefully protected to ensure the individual's privacy is maintained.

Scope:

In this context, the following are defined as:

An **Individual** is any client, representative of a client, employee, visiting health professional, or visitor to Alicaring Community.

Alicaring Community maintains that privacy and confidentiality can be maintained by:

- Collecting only the information required under State and Federal legislation to deliver the service;
- Ensuring openness and consultation with individuals concerning the information collected;
- Providing individuals with access to their health and other records;
- Ensuring anonymity, where possible, and when requested by the individual;
- Disclosing personal information to other parties only with the consent of the individual or where it is legally or ethically justified; and
- Ensuring secure storage of information.

Relevant Legislation

- Aged Care Act 2024 (Cth)
- Aged Care Quality Principles 2014 (Cth)
  - User Rights Principles 2014
  - Quality of Care Principles 2014
  - Accountability Principles 2014
  - Information Principles 2014
  - Records Principles 2014
- Crimes Act 1914
- Electronic Transmission Act 1999
- Evidence Act 1995
- Health Legislation Amendment Bill 2019
- Privacy Act 1988 (amended by the Privacy Amendment (Private Sector) Act 2000)
- Work Health and Safety Act 2011 (QLD)
  - Work Health and Safety Regulation 2011 (QLD)

Other Relevant Documents

- Aged Care Quality Standards
- Charter of Aged Care Rights
- Department of Health and Aged Care August 2023– Support at Home Program – Operational Manual

Protocols

COLLECTION OF PERSONAL INFORMATION

1. Alicaring Community will only collect the personal information required to comply with State and Federal legislation for the delivery and funding of the clients' care and lifestyle needs, the employment of staff, or as otherwise required to provide aged care services.
2. Individuals will provide their personal information or be made aware of and agree to access personal information from other sources.
3. Alicaring Community will provide the individual with information regarding the purpose and use of the personal information required and who will have access to the information.
4. Individuals will be informed of their right to withhold information or provide information anonymously, if applicable.
5. Individuals will be informed of the complaints mechanism should they wish to lodge a complaint about how Alicaring Community manages their personal information.

PROTECTION OF PERSONAL INFORMATION

1. Individuals will be informed of Alicaring Community's responsibilities concerning the protection of personal information through:
    a. Handbooks;
    b. Brochures;
    c. Contracts/service agreements; and
    d. Policies and procedures.
2. All employees and volunteers will be required, on commencement of service, to sign a *Confidentiality Agreement.*
3. Employees will provide no personal information over the telephone unless established that the caller has legitimate grounds to access information and can give proof of identity.
4. The Director/ Chief Executive Officer or the Support at Home Manager are the only individuals authorised to divulge employee information, where it is legally and ethically justified. They may nominate another employee of Alicaring Community to provide this information in their absence in particular circumstances.
5. No personal information about anyone except the name of the caller should be left on voicemail.
6. Personal information may only be faxed in circumstances where it is urgently required, and only then can the viewer guarantee the confidentiality and security of the information. All facsimiles must be accompanied by Alicaring Community's cover sheet, which carries a privacy warning. Wherever possible, documents should be scanned and emailed to the individual requesting the information.
7. Personal information will not be sent by email unless all identifiers have been removed or encrypted.
8. Employees are advised to avoid having personal mail addressed to their place of work.
9. The Administrative Officer is the designated person who opens the mail. All mail will be date stamped on receipt prior to distribution.
10. Mail and facsimiles addressed:
    a. To a client will only be opened by the client and/or person(s) responsible
    b. By title or position alone will be opened by the designated mail opener
    c. "Personal" or "confidential" will be opened only by the addressee
    d. By title or position only and marked "personal" or "confidential" will be opened by the person occupying that position or by the person acting in the position.
    e. To Alicaring Community will only be opened by the designated mail opener and forwarded to the Director/ Chief Executive Officer.

11. Outgoing mail containing information subject to the *Privacy Act* 1988 will be sent in a sealed envelope, addressed to an individual by name and marked "confidential". If couriered, the envelope/parcel will be sealed with a sticker over the opening that is marked "confidential".
12. Personal information should not be copied unless it is essential to do so.
13. The anonymity of clients and/or employees will be maintained during case presentations, research activities, seminars, and conference presentations.
14. Fictitious data should be used for all training and demonstration purposes.
15. Consent will be obtained to utilise photographs, slides and other visual aids that identify individuals.
16. Personal information related to clients and/or employees will not be discussed in public areas or with individuals who are not directly involved with the client's care or the employee's supervision.
17. All paper-based clinical records pertaining to current clients will be securely stored in the designated offices. Access to electronic clinical records will be limited to appropriate individuals who have been issued with a secure password.
18. All paper-based employee records pertaining to current employees will be securely stored in the Director/Chief Executive Officer's office. Access to electronic employee records will be limited to appropriate individuals who have been issued a secure password.
19. All non-clinical data (agreements, asset declarations etc.) will be stored separately to clinical records and held in the Quality Coordinator's office and only accessed by the Director/Chief Executive Officer, Support at Home Manager, and administrative staff involved with client agreements and accounts.

MEDIA

1. No information regarding a client, employee, visiting health professional, service provider or Alicaring Community will be disclosed to the media by an employee.
2. No information is to be provided by any staff member to the media, even if it is 'off the record'.
3. A short file note should be prepared by the Worker summarising the nature of any media inquiry and the information provided in response to any media inquiry and given to the Director/Chief Executive Officer.
4. Requests from the media for information will be referred to the Director/ Chief Executive Officer, who will determine what information will be provided. The decision will be based on consideration of:
    a. Consent from the relevant parties;
    b. Possible legal implications; and
    c. Ramifications to relevant individual(s) and/or Alicaring Community.

ACCESS TO RECORDS

1. Access to clinical records (paper-based and electronic) is restricted to healthcare personnel currently involved in the care, observation, assessment, diagnosis, professional advice and management of the client, and other circumstances as described under Protocol "Authorised Disclosure".
2. Individuals will be made aware of their right to access their internal records and the process for doing so.
3. Through written application to the Director/Chief Executive Officer of Alicaring Community, individuals may request access to their clinical records. As soon as practicable on receipt of the application, the Director/ Chief Executive Officer will make the clinical record available to the on-site and in the presence of the Support at Home Manager to assist with interpretation of the record.

    The Director/ Chief Executive Officer may refuse a request by an individual for access to their clinical record:

   a. If the medical practitioner in charge of the persons care advises that the request should be refused; and/or
   b. If the Director/Chief Executive Officer is satisfied that access by the client and/or person(s) responsible would be prejudicial to the client's physical or mental health.
4. The application to the Director/Chief Executive Officer for the request to access the clinical record will be retained in the client's clinical record.
5. An individual is entitled to dissent from or add to the clinical record. Their comments will be attached, as an addendum, to the record, along with an explanation of the circumstances.
6. Access to employee records (paper-based and electronic) is restricted to the Director/ Chief Executive Officer and their representative and designated administrative staff involved in human resource management activities and other circumstances as described under Protocol "Authorised Disclosure".
7. An employee is entitled to access their records and to obtain a copy of any document therein. In these circumstances, access will be on-site and in the presence of the Director/Chief Executive Officer.
8. An employee is entitled to dissent from or add to their employee record. The employee's comments will be attached, as an addendum, to the record, along with an explanation of the circumstances.
9. Client medical and care records and staff records must be retained for a minimum of seven (7) years. Destruction must then be first authorised by the Support at Home Manager or equivalent in consultation with the Quality Coordinator.
10. Confidential information should be shredded before disposal for security purposes.
11. Where an external service provider destroys confidential records, an agreement will be entered into by both parties.

AUTHORISED DISCLOSURE

1. Personal information regarding a client or employee may be disclosed:
   a. When valid informed consent is obtained from the individual for disclosure of specific information for a particular purpose;
   b. When an employee believes disclosure is necessary for the interests of public safety. In this situation, the employee should contact the Director/ Chief Executive Officer or their representative; and
   c. Where there is an obligation under the *Crimes Act* 1914 to notify police about serious criminal offences (including drug trafficking, serious assaults or murder and manslaughter).
2. Information will be provided to government authorities who have specific statutory powers to demand access to information. In these circumstances, the Director/ Chief Executive Officer will be responsible for responding to the subpoena promptly and will:
   a. Obtain the precise authority of the person requesting access, including reference to the Section of the Act under which access is authorised;
   b. Obtain the nature of the access requested to ensure that only material relevant to the statutory demand is released; and
   c. Bring the subpoena to the attention of a legal expert.

   This information will be recorded and stored in the client's, employee's or other relevant files.

3. The use and disclosure of health information for secondary purposes (For example, research or collection of data for government departments) will be in accordance with the Health Privacy Principles 10(1)(d) and 11(1)(d).

NOTIFICATION OF ELIGIBLE DATA BREACHES

1. An Eligible Data Breach happens if:

   a. There is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
   b. The access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.
2. Alicaring Community must notify the affected individual(s) or organisation(s) (affected individuals) and the Office of the Australian Information Commissioner (OAIC) if:
   a. There are reasonable grounds to believe that an eligible data breach has happened; or
   b. Alicaring Community is directed to do so by the OAIC.
3. All Workers are responsible for reporting an actual or suspected data breach to the Support at Home Manager or their supervisor.
4. The Support at Home Manager or supervisor is responsible for taking immediate steps per the Data Breach Response Plan (Annexure 1), including:
   a. Recording the reported breach using Part 1 of the Data breach report form (Annexure 3);
   b. Taking immediate steps to contain the breach; and
   c. Notifying the Director/ Chief Executive Officer.
5. The Director/ Chief Executive Officer or delegate is responsible for investigating, assessing and responding to the data breach following the Data breach response plan (Annexure 1), including:
   a. Completing the Data breach matrix (Annexure 2);
   b. Completing Part 2 of the Data breach report form (Annexure 3); and
   c. Determining whether the breach is required to be notified and ensuring the relevant parties are notified.
6. If Alicaring Community is required to notify affected individuals of an Eligible Data Breach, Alicaring Community will do so by using the Template notification letter to individuals at risk (Annexure 4). The notification to affected individuals will include:
   a. Alicaring Community's identity and contact details;
   b. A description of the data breach;
   c. The kinds of information concerned; and
   d. Recommendations about the steps that individuals should take in response to the serious data breach.
7. There are several exceptions to notification that may apply depending on the circumstances. These include:
   a. If compliance with the notification requirements would be inconsistent with another law of the Commonwealth that regulates the use or disclosure of information, Alicaring Community will be exempt to the extent of the inconsistency;
   b. If compliance would be inconsistent with another law of that kind prescribed in regulations under the Privacy Act;
   c. If the notification requirements in the My Health Records Act 2012 apply, then Alicaring Community will be exempt to avoid double notification;
   d. If Alicaring Community has taken remedial action following an Eligible Data Breach or potential Eligible Data Breach and a reasonable person would conclude that as a result of the remedial action, the unauthorised access or unauthorised disclosure of personal information (including unauthorised access or unauthorised disclosure following a loss of the information) is not likely to result in serious harm to the affected individuals, or remedial action has prevented a loss of information from leading to unauthorised access or disclosure;
   e. If remedial action following access or disclosure would lead a reasonable person to conclude that only particular individuals within a broader group are not likely to be at risk of serious harm following the remedial action, then Alicaring Community will not be required to notify those particular individuals (but would still be required to notify the remainder of the individuals); and

f. Suppose the Commissioner has (at the request of Alicaring Community or the Commissioner's own initiative) exempted Alicaring Community from providing notification of an Eligible Data Breach because the Commissioner is satisfied that it is reasonable in the circumstances to do so. In that case, Alicaring Community may be exempt altogether or for some time.

8. Staff who fail to comply with this Data breach response policy may face disciplinary action and, in serious cases, termination of employment.