PRIVACY AND CONFIDENTIALITY POLICY AND PROCEDURE

1.0 PURPOSE AND SCOPE

Concentric keeps full and accurate records for each client, including the activities and decisions related to each client.

To ensure that management of clients' personal information meets all relevant legislative and regulatory requirements, this policy sets out the requirements, roles and responsibilities for ensuring compliance with the legislation and the benefits of good record keeping practices.

All staff are required to comply with this policy and failure to comply may result in disciplinary action. This policy and procedure applies to current and potential clients, their carers and family members. The policy applies to records in all formats, including digital/electronic and hard copy records.

2.0 DEFINITIONS

Personal information – Recorded information (including images) or opinion, whether true or not, from which the identity (including those up to thirty years deceased) could be reasonably ascertained.

Sensitive information – Information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political party, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preference or practices, or criminal record. This is also considered to be personal information.

Health information – Any information or an opinion about the physical, mental or psychological health or ability (at any time) of an individual.

Information Privacy – refers to the control of the collection, use, disclosure and disposal of information and the individual's right to control how their personal information is handled.

3.0 POLICY

Concentric is committed to the transparent management of personal and health information about its clients and staff.

This commitment includes protecting the privacy of personal information, in accordance with the Australian Privacy Principles (APPs) set out in the *Privacy Act 1988 (Cwlth)* amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cwlth)*.

4.0 PROCEDURE

PERSONAL INFORMATION

Concentric uses Lumary and Skedulo as its principal client systems. The systems are used to register, capture and track hardcopy documents and digital files whether received, generated or acted upon by the Staff. Access to the systems and user training is available to all staff and forms part of the induction training.

Concentric ensures the following information should be recorded in our principal client systems:

- name,
- date of birth,
- gender,
- current and previous addresses,
- residency status,
- telephone numbers and e-mail addresses,
- details of who the client would like contacted in the unlikely event of a medical emergency,
- medical history or information provided by a health service provider.

Furthermore, the client's file may include:

- bank account/credit card details (with encryption),
- the therapists observations, clinical findings or assessments and any "working diagnoses",
- Therapy goals, proposed plan of care, associated risks and alternatives (if any) discussed with the client.
- tax file number,
- driver's licence number,
- Medicare, NDIS, DVA, MVA Private Health Insurance details,
- Centrelink information,
- photographs,
- race or ethnicity,
- the client's consent to the agreed plan of care and proposed fees;
- all 'care' provided and the client's response to that care, including achievements/therapy outcomes,
- any advice, instructions or warnings given to the client and a simple plan for the next session.
- Details of any further exchanges with the client, or their carer, occurring via telephone, email etc.
- medical history or information provided by other health services or practitioners.

In collecting personal information, Concentric will inform the client:

- that information is being collected;
- the purposes for collection;
- who will have access to the information;
- the right to seek access to, and/or correct, the information; and
- the right to make complaint or appeal decisions about the handling of their

information.

Client information is used to:

- assess and provide services;
- administer and manage those services;
- evaluate and improve those services;
- contribute to research;
- contact family, carers, or other third parties if required; and
- meet our obligations under the NDIS.

Clients are to be provided with the *Client Consent Form or Permission to Share and Obtain Information Form* at the time of commencing service with Concentric. This form is to be:

- signed and placed in the client's file;
- held securely with access limited to staff members in the performance of their role.

The purpose of clinical records is to ensure the safety and continuity of client care and to record their journey from start to finish.Carefully recording the sequence of events allows practitioners to return to the records at any time to clarify the facts behind treatment and any decisions made. Clear clinical records are essential for fulfilling the obligations to such entities such as government agencies and private health funds. Accurate records also assists in defending a claim of negligence or misconduct.

CONSENT

Consent must be voluntary, informed, specific and current.

Voluntary consent: A person must be free to exercise genuine choice about whether to give or withhold consent. This means they haven't been pressured or coerced into make a decision, and they have all the information they need in a format they understand. Voluntary consent requires that the person is not affected by medications, other drugs or alcohol when making the decision.

Informed consent: A person's capacity to make decisions will vary depending on the type of decision or its complexity, or how the person is feeling on the day. The way information is provided to a person will also affect his or her capacity to make decisions. Choices must be offered in a way that the person understands, for example by using images or signing.

Support, where required, must be provided for the person to communicate their consent.

Specific consent: Consent must be sought for a specific purpose and this purpose must be understood by the client.

Current consent: Consent cannot be assumed to remain the same indefinitely, or as the person's circumstances change. People and guardians are entitled to change their minds and revoke consent at a later time.

COLLECTION, ENTRY AND STORAGE OF PERSONAL INFORMATION

Clinical records include both, hard copy or digital/electronic information pertaining to the individual's care.

Any hard copy or paper documentation must be scanned into the relevant client file as soon as possible and not more than 24 hours after the activity occurred.

The hard copies are to be shredded once the copies have been scanned unless requested to be kept by the client or practitioner. Kept files are to be stored in a local area for 7 years as per above mentioned Privacy Legislation.

All digital/electronic records are to be entered into the system as soon as possible and not later than 24 hours after the activity occurred. Failure to complete entries within the client systems and delete off any standalone computer (used while the file may be active) within the 24 hour time-frame may result in disciplinary action.

Concentric collects information:

- directly from clients orally or in writing;
- from third parties, such as medical practitioners, government agencies, client representatives, carer/s, and other health service providers;
- from client referrals; and
- from publicly available sources of information.

Concentric will collect sensitive information:

- only with client consent, unless an exemption applies: e.g. the collection is required by law, court/tribunal order or is necessary to prevent or lessen a serious and imminent threat to life or health;
- fairly, lawfully, and non-intrusively;
- directly from client, if doing so is reasonable and practicable;
- only where deemed necessary to support
    - service delivery to clients;
    - staff activities and functions; and
- giving the client the option of interacting anonymity, if lawful and practicable.

Concentric takes all reasonable steps to protect personal information against loss, interference, misuse, unauthorised access, modification, or disclosure. Concentric will destroy, or permanently de-identify personal information that is

- no longer needed;
- unsolicited and could not have been obtained directly; or
- not required to be retained by, or under, an Australian law or a court/tribunal order.

Concentric has appropriate security measures in place to protect stored electronic and hard-copy materials. Concentric has an archiving process for client files which ensures files are securely and confidentially stored and destroyed in due course.

Should a breach in privacy occur, potentially exposing client information (e.g. computer system hacked, laptop stolen etc.) the executive team will immediately act to rectify the breach in accordance with organisational policy and processes.

UPDATING CLIENT INFORMATION

To ensure that client information is accurate, complete, current, relevant and not

misleading, Concentric checks personal details and updates client files accordingly:

- whenever reviewing a client's service; and / or
- upon being informed of changes or inaccuracies by clients or other stakeholders

There will be no charge for any correction of personal information.

Where Concentric has previously disclosed client personal information to other parties, should the client request us to notify these parties of any change to their details, we must take reasonable steps to do so.

USE AND DISCLOSURE OF INFORMATION

Concentric respects the right to privacy and confidentiality, and will not disclose personal information except where we need to:

- Protect your health and safety, or the health and safety of others
- Provide our services to you
- Comply with legal obligations
- Enforce our rights or protect our business

For these purposes, Concentric may disclose your personal information to other people, organisations or service providers, including:

- Healthcare providers involved in your care
- A "person responsible" if you are unable to give or communicate consent (e.g. next of kin, carer, or guardian)
- Your authorised representatives (e.g., legal advisors, guardians)
- Our professional advisers, (e.g. lawyers, accountants, auditors)
- Recruitment agencies
- Government agencies (e.g. Centrelink, ATO, NDIA, other government agencies)
- Third-party service providers (e.g. business support teams based in the Philippines)
- Organisations undertaking research where information is relevant to public health or public safety; and
- When required or authorised by law

If there is a change of control in one of our businesses (whether by merger, sale, transfer of assets or otherwise) customer information, which may include your Personal Data, could be disclosed to a potential purchaser under a confidentiality agreement. We would only disclose your information in good faith and where required by any of the above circumstances.

ACCESSING PERSONAL INFORMATION

Clients can request and be granted access to their personal information, subject to exceptions allowed by law.

Requests to access personal information must state the:

- information to be accessed
- preferred means of accessing the information,

and should be forwarded to the Team Leader either verbally, or in writing to the specific clinic's email address or postal address.

The Team Leader will assess the request to access information, taking into consideration current issues that may exist with the client, and whether these issues relate to any lawful exceptions to granting access to personal information.

Should the Team Leader decide that access to personal information will be denied, they must, within 30 days of receipt of the request, inform the client in writing of the:

- reasons for denying access and
- mechanisms available to complain or appeal.

Should access be granted, the Team Leader will contact the client within 30 days of receipt of the request to arrange access to their personal information.

Should Concentric be unable to provide the information in the means requested, the Team Leader will discuss with the client alternative means of accessing their personal information.

Reasonable charges and fees, incurred by Concentric in providing the data as requested, may be passed on to the client.

Concentric takes all reasonable steps to protect personal information against loss, interference, misuse, unauthorised access, modification, or disclosure. Concentric will destroy, or permanently de-identify personal information that is

- no longer needed;
- unsolicited and could not have been obtained directly; or
- not required to be retained by, or under, an Australian law or a court/tribunal order.

HOW WE PROTECT YOUR PERSONAL INFORMATION

At Concentric, we are committed to protecting your personal information by partnering with trusted third-party service providers and implementing strong user security measures. We utilise Software as a Service (SaaS) platforms which enforce industry-standard security practices, including encryption and secure networks.

To further safeguard your data, we require the use of strong passwords, multi-factor authentication (MFA) for all authorised personnel accessing our systems and restricted administrative access. We enforce patching of computers with robust monitoring and reporting.

Our IT service providers are selected to fully comply with all Australian privacy laws and implement robust safeguards to protect against unauthorised access, loss, misuse, or disclosure of your data.

DATA BREACH

Concentric has established policies and procedures for addressing suspected privacy breaches. We will investigate any suspected breaches to identify the cause and implement corrective measures. Where required, we will notify affected individuals and the Office of the Australian Information Commissioner.

COMPLAINTS

Questions or concerns about Concentric' privacy practices should be brought, in the first instance, to the local clinic's management attention.

Clients may directly email the executive team at support@concentric.com.au

In investigating the complaint Concentric may, where necessary, contact the client making the complaint to obtain more information.

The client will be advised either in writing, or in a face to face meeting, of the outcomes and actions arising from the investigation.

If concerns cannot be resolved and clients wish to formally complain about how their personal information is managed, or if they believe Concentric has breached an Australian Privacy Principle (APP) and/or an Information Protection Principle (IPP), they may send their concerns to:

> The Office of the Australian Information Commissioner
>
> Phone: 1300 363 992
>
> Web: http://www.oaic.gov.au (online complaint form)
>
> Email: enquiries@oaic.gov.au

Any complaint about services delivered under the NDIS may be brought to the NDIS Quality and Safeguards Commission.

Complaints to the NDIS Commission can be lodged via:

- web: https://www.ndiscommission.gov.au/
- email: feedback@ndis.gov.au
- phone: 1800 035 544 (free call from landlines) or TTY 133 677. Interpreters can be arranged.

End of policy document. Uncontrolled when printed.