PRIVACY AND CONFIDENTIALITY POLICY AND PROCEDURE

Policy Code	**CAP001.01**
Person Responsible	**Director**
Status (Draft/Released)	**Released**
Date Last Updated	**6 APRIL 2023**

1.0 PURPOSE AND SCOPE

To ensure that management of personal information for clients meets all relevant legislative and regulatory requirements.

This policy and procedure applies to current and potential clients, their carers and family members.

2.0 RISK

Because people with disabilities are more vulnerable to exploitation and abuse than others in the community, workers with access to client information automatically occupy risk-assessed roles under the NDIS Commission.

The primary risk to privacy and confidentiality arises from the collection, storage and sharing of client information. Access by non-authorised persons may expose clients to risk. Safe storage and access policy protects clients from abuse and exploitation. This policy addresses these issues.

There is a risk that information will be shared inadvertently and without the intention to do harm. Information may be unintentionally disclosed by careless use of tablet- or phone-based software, shared with a client's supporters against the client's wishes, or disclosed to peers on the assumption that the information is publicly known. Cultural assumptions around sharing information are diverse and change rapidly. Social media platforms may allow clients to be identified. This risk may be minimised by:

- raising staff awareness of privacy and confidentiality
- ensuring consent is obtained before gathering data (including audio and photographic data)
- ensuring that consent is specific to the use of data, and that consent is current
- encouraging clients to provide feedback and complaints about the use of their information.

These issues are addressed in this policy.

3.0 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.

4.0 POLICY

Kindred Health Group 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)* and in accordance with the *Privacy Policy*, Department of Human Services, endorsed June 2002 (amended August 2005) (Vic), the *Health Records Act 2001 (Vic)*, the *Information Privacy Act (2000) (Vic)*, and the *Freedom of Information Act 1982 (Cwlth)*.

Kindred Health Group's *Privacy and Confidentiality Policy and Procedure* is made publicly available.

5.0 PROCEDURE

Personal information

- Personal information may include:
  - name,
  - date of birth,
  - gender,
  - current and previous addresses,
  - residency status,
  - telephone numbers and e-mail addresses,
  - bank account details,
  - tax file number,
  - driver's licence number,
  - Centrelink information,
  - photographs,
  - race or ethnicity, and
  - medical history or information provided by a health service.

- In collecting personal information, Kindred Health Group 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.

Client Consent

- Clients are to be provided with the *Client Consent Form* at the time of commencing service with Kindred Health Group. 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.

Updating Client Information

- To ensure that client information is accurate, complete, current, relevant and not misleading, Kindred Health Group 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 Kindred Health Group 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.

Collection and Storage of Personal Information.

- Kindred Health Group 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.

- Kindred Health Group 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.
- Kindred Health Group takes all reasonable steps to protect personal information against loss, interference, misuse, unauthorised access, modification, or disclosure. Kindred Health Group 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.
- Kindred Health Group has appropriate security measures in place to protect stored electronic and hard-copy materials. Kindred Health Group 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 Director will immediately act to rectify the breach in accordance with organisational policy and processes.

Disclosing information

- Kindred Health Group respects the right to privacy and confidentiality, and will not disclose personal information except:
  - where disclosure would protect the client and / or others;
  - where necessary for best service practice; or
  - where obligated by law.
- For these purposes, Kindred Health Group may disclose clients' personal information to other people, organisations or service providers, including:
  - medical and allied health service providers who assist with the services we provide to clients;
  - a 'person responsible' if the client is unable to give or communicate consent e.g. next of kin, carer, or guardian;

- the client's authorised representative/s e.g. legal adviser;
- our professional advisers, e.g. lawyers, accountants, auditors;
- government and regulatory authorities, e.g. Centrelink, government departments, and the Australian Taxation Office;
- organisations undertaking research where information is relevant to public health or public safety; and
- when required or authorised by law.

- Any information released for evaluation or research purposes will be de-identified.
- Note that consent is not required to share information to promote the safety and wellbeing of a child for organisations that fall under Victoria's Child Information Sharing Scheme.

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
  - the preferred means of accessing the information,
  - and should be forwarded to the Director either verbally, or in writing to:

    Postal: 10 Little Dryburgh St South, North Melbourne VIC 3051

    Phone: 0411 858 409

    Email: hello@kindredhealthgroup.com.au
- The Director 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 Director 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
  - the mechanisms available to complain or appeal.
- Should access be granted, the Director will contact the client within 30 days of receipt of the request to arrange access to their personal information.
- Should Kindred Health Group be unable to provide the information in the means requested, the Director will discuss with the client alternative means of accessing their personal information.
- Reasonable charges and fees, incurred by Kindred Health Group in providing the data as requested, may be passed on to the client.

Complaints

- Questions or concerns about Kindred Health Group's privacy practices should be brought, in the first instance, to the Director's attention.
- Clients may directly email the Director at hello@kindredhealthgroup.com.au
- In investigating the complaint Kindred Health Group 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 Kindred Health Group has breached an APP and/or IPP, they may send their concerns in writing to:
  - Office of the Victorian Information Commissioner

    Email: privacy@cpdp.vic.gov.au

    Phone: 1300 666 444

    or through the online form available at

    https://www.cpdp.vic.gov.au/menu-privacy/privacy-public/privacy-public-make-complaint

Breaches of Privacy

- Kindred Health Group are required to disclose a data breach to the Office of Australian Information Commissioner if the data contains personal information that is likely to result in "serious harm", which includes any of the following: physical, psychological, financial or reputational harm. Personal information is information about an identified individual, or an individual who is reasonably identifiable.
- Any staff who identify a potential breach must immediately inform their line manager, who must report to the Director for further action.

POLICY AMENDMENT RECORD		
DATE	BRIEF DESCRIPTION OF AMENDMENT	AUTHORISED