



Purpose

InSyncCS is committed to respecting people's right to be afforded individual privacy, dignity, and confidentiality, and to ensure that our management of personal client information meets all relevant legislative and regulatory requirements.

Scope

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

Definitions

- **Privacy** - a state in which one is not observed or disturbed by other people. A breach of privacy occurs when there is a failure to comply with one or more of the privacy principles set out in the Information Privacy Act 2009.
- **Dignity**- the state or quality of being worthy of honour or respect. Dignity is the right of a person to be valued and respected for their own sake, and to be treated ethically. If people feel their identity and value as a human being is not respected, this can stop them from enjoying life and living comfortably. Upholding the dignity of individuals means our approach to the way we support someone promotes and does not undermine a person's self-respect regardless of any difference.
Dignity is:
 - concerned with how people feel, think, and behave in relation to the worth or value of themselves and others.
 - Dignified support, or the lack of it, can have a profound effect on people's well-being.
 - the result of being treated with respect and is internal to everyone, and is often associated with a sense of worth, well-being or a sense of purpose.
 - Dignity and respect is important to every one of us and a key part of our role is about ensuring the people we support are treated in ways we expect to be treated.
- **Confidentiality** - the state of keeping or being kept secret or private. A breach of confidentiality occurs when data or information provided in confidence by a client is disclosed to a third party without consent.
- **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 orientation 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.
- **Breach of Privacy and Confidentiality** - Breaches of privacy and confidentiality can be:
 - Providing written information not in accordance with guidelines.
 - Providing verbal information not in accordance with guidelines.
 - Discussing personal information of people supported and/or other staff with or in front of other people.

Approved By: InSyncCS Director		Version: 1.01		Created by: Jennifer Manwaring	
Approval Date	Jan 2020	Implementation Date	Aug 2024	Review Date	Aug 2027



Policy

The policy of InSyncCS is to ensure the individual privacy, dignity and confidentiality is maintained for clients, staff, contractors and visitors of this service.

InSyncCS will prevent unauthorised persons gaining access to an individual's confidential records and permit individuals' access to their own records.

Procedure

Privacy and dignity will be understood to include respect for the person's physical body, personal space, and belongings, living arrangements, and personal information shared with informed consent. People receiving services from InSyncCS are entitled to the same level of privacy as all other members of society.

The people we support are entitled to:

- enjoy a private space
- feel comfortable and reassured that their personal information and belongings will be respected
- communicate confidentially with friends, family, and carers when they wish to do so
- be supported in such a way that their personal dignity is maintained
- wherever possible, make choices about those involved in their daily lives.

When supporting people dignity is about:

- being polite and respectful
- being thoughtful and caring
- actively engaging people in their daily activities and choices
- keeping people informed
- meeting their individual needs
- ensuring their privacy and modesty and not treating people as an object of service

Staff Responsibility

All staff have a responsibility to:

- Ensure client's personal information is not left on desks or photocopiers and that records and information are securely locked away.
- Ensure client information is stored on InSyncCS 'Halaxy'(1) only, and not on the desktop of individual computers.
- Ensure that personal information collected or disclosed is accurate, complete, and up-to-date, and provide access to any individual and/or their families to review information or correct wrong information about themselves
- Only collect the necessary information from people and their families/carers.
- Ensure conversations of a personal nature are conducted away from public areas.
- Do not share client or staff private or confidential information or photographs through external social media platforms unless permission has been explicitly given and documented.
- Ensure clients are aware of their rights regarding access to documents and files
- Ensure that people know what sort of personal information is held, what purposes it is held it for and how it is collected, used, disclosed and who will have access to it
- Consider the implications and risks of forwarding email messages to a third party without consent.
- If sending information of a private nature, notify the recipient that confidential information is about to be sent.
- Respect people's dignity always.

All staff are responsible for the management of personal information to which they have access.

All people supported and/or their families/carers are given the policy on Information Privacy and Confidentiality.

Written consent must be gained and documented to share any information.

Approved By: InSyncCS Director		Version: 1.01		Created by: Jennifer Manwaring	
Approval Date	Jan 2020	Implementation Date	Aug 2024	Review Date	Aug 2027



Privacy, Dignity and Confidentiality Policy and Procedure and Agreement Form

Formal conversations about people must take place in a private setting between the relevant parties, and never in a public place.

All employees acknowledge that they understand through signing the employment contract, that they owe InSyncCS, its employees, workers and clients, a duty of privacy, dignity and confidentiality and that they will not, at any time, knowingly disclose to any unauthorised personnel confidential information that comes to their knowledge during or following cessation of their employment, including documents, materials, processes, and data whether physical, electronic or any form.

Explaining Confidentiality to Clients

All clients must be advised of their right to confidentiality, at their initial consultation/interview/service assessment

Clients must be advised of:

- The personal information InSyncCS will need to collect and why.
- How the information will be stored?
- Who will have access to this information?
- How the collection of this personal and health information will benefit the client’s health and wellbeing? What information is used for Reporting?

All clients must give written consent before any of their personal or health information may be shared with any other party. If this consent is not given then the information cannot be released by InSyncCS

All clients have the right to refuse to share any personal information with InSyncCS staff or any other person or organisation.

All staff, and Contractors must be given access to the relevant "Acts" as listed above and read the relevant policies and procedure on Confidentiality and sign a Confidentiality Agreement. Completed Agreements will be stored in personnel or appropriate file.

Privacy, Dignity, and Confidentiality Violations

Violations will result in disciplinary action against the offending individual which may include termination of employment or legal action may be taken.

Staff must ensure when working with vulnerable people that:

- they strictly adhere to this policy.
- a person’s right to dignity is upheld.
- sharing of confidential information only where it is in the best interests of the individual and if they have given consent in line with the Information Privacy Act 2000.
- standard sharing of information regarding people supported takes place between staff and must be done in a formal manner. Such information disclosed will be relevant to daily activities and support requirements and associated health and wellbeing issues.
- any information sharing that is outside of what is relevant to the person's involvement with InSyncCS, either directly or indirectly, is not appropriate and may be considered a breach of privacy and/or confidentiality.
- Always work strictly within the legal guidelines (Refer to References at end of document).

Personal information and Consent

Personal information includes details that identify an individual directly or indirectly, such as name, address, phone number, email, and date of birth. Sensitive information, a subset of personal information, can include details about a

Approved By: InSyncCS Director		Version: 1.01		Created by: Jennifer Manwaring	
Approval Date	Jan 2020	Implementation Date	Aug 2024	Review Date	Aug 2027



Privacy, Dignity and Confidentiality Policy and Procedure and Agreement Form

person’s racial or ethnic origins, political or religious beliefs, sexual orientation, health or genetic information, family court orders, or criminal record, the misuse of which could lead to discrimination or embarrassment.

Clients are provided with the Client Consent Form at the time of commencing service with InSyncCS. 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.

Personal information may include:

- name
- date of birth
- gender
- gender preferences
- current and previous addresses
- telephone numbers and e-mail addresses
- bank account details
- photographs
- race or ethnicity
- medical history or information provided by a health service.

Why we collect personal information

The sharing of personal information with InSyncCS enables us to assess and support our clients in addressing their concerns. Personal information is retained to help us provide an informed service. Due to our duty of care, anonymity is not feasible; however, clients may use a pseudonym, although a legal name is required for record-keeping purposes.

In collecting personal information, InSyncCS 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.

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.

Updating Client Information

To ensure that client information is accurate, complete, current, relevant, and not misleading, InSyncCS checks personal details and updates client files accordingly:

- whenever reviewing a client’s service; and / or

Approved By: InSyncCS Director		Version: 1.01		Created by: Jennifer Manwaring	
Approval Date	Jan 2020	Implementation Date	Aug 2024	Review Date	Aug 2027



- upon being informed of changes or inaccuracies by clients or other stakeholders

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

We collect personal information through various methods, including:

- 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.
- Information verbally shared during sessions
- Written communications received via email, SMS, or letter
- Our online booking system
- Our intake form
- Social media interactions
- Guardians providing information for clients under 18
- Referrals from GPs or other healthcare practitioners

InSyncCS 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.

Storage of Personal Information

To safeguard personal information, we use secure storage methods accessible only by approved personnel. Information may be stored as hard copies, on secure servers, or offline. We do not retain credit card or banking details once payment is processed and periodically dispose of unnecessary information securely, in accordance with legal obligations. If a security breach is identified, we will investigate and take remedial action, notifying affected individuals as required by the Privacy Act.

InSyncCS takes all reasonable steps to protect personal information against loss, interference, misuse, unauthorised access, modification, or disclosure. InSyncCS 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.

Approved By: InSyncCS Director		Version: 1.01		Created by: Jennifer Manwaring	
Approval Date	Jan 2020	Implementation Date	Aug 2024	Review Date	Aug 2027



Integrity of Your Personal Information

We endeavour to keep personal information accurate and up to date. Clients may request updates or corrections to their information, which we will handle in compliance with the Privacy Act. Should a breach in privacy occur, potentially exposing client information (e.g. computer system hacked, laptop stolen etc.) the Directors will immediately act to rectify the breach in accordance with organisational policy and processes.

InSyncCS has appropriate security (2) measures in place to protect stored electronic and hard-copy materials. InSyncCS has an archiving process for client files which ensures files are securely and confidentially stored and destroyed at the proper time.

Disclosing information

InSyncCS 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, InSyncCS 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.

Disclosure of Your Personal Information

We will not disclose personal information to third parties without consent unless required by law. It is unlikely that information will be shared with parties outside Australia. Any information released for evaluation or research purposes will be de-identified.

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

Requests to access personal information must state:

- the information to be accessed
- the preferred means of accessing the information
- must be forwarded to the Directors in writing to: enquiries@insyncnccs.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.

Approved By: InSyncCS Director		Version: 1.01		Created by: Jennifer Manwaring	
Approval Date	Jan 2020	Implementation Date	Aug 2024	Review Date	Aug 2027



Privacy, Dignity and Confidentiality Policy and Procedure and Agreement Form

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 Directors will contact the client within 30 days of receipt of the request to arrange access to their personal information.

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

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

Complaints about Breaches of Privacy and/or Confidentiality

Questions or concerns about InSyncCS privacy practices should be brought, in the first instance, to the Directors' attention – Refer to Complaints Policy. If concerns cannot be resolved and clients wish to formally complain about how their personal information is managed, or if they believe InSyncCS has breached an APP and/or IPP, they may send their concerns in writing to: enquiries@insynccs.com.au.

If you believe your personal information has not been managed in accordance with the Privacy Act, please contact us directly. We will investigate and attempt to resolve the matter promptly. If unsatisfied with our response, you may file a complaint with the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.

Changes to This Privacy Policy

We may update this privacy policy occasionally and will inform clients of changes via email or our website.

Contact Us

If you have any questions regarding privacy matters, please contact us at jennifer@insynccs.com.au

InSync Counselling and Support (InSyncCS)

Address 490 Ebdon Street Albury NSW 2640

Mobile 0429112752

Email jennifer@insynccs.com.au

Web www.insynccs.com.au

Related documents

- Disciplinary Policy & Procedure
- Record Keeping Policy & Procedure
- Decision making and Informed Choice Policy & Procedure
- Aboriginal and Torres Strait Islander People Policy and Procedure
- Person Centered Supports Policy and Procedure
- Participants Rights & Responsibilities Policy and Procedures
- Advocacy policy and Procedure
- Managing Occupational Risk in the Community Setting

Approved By: InSyncCS Director		Version: 1.01		Created by: Jennifer Manwaring	
Approval Date	Jan 2020	Implementation Date	Aug 2024	Review Date	Aug 2027



Privacy, Dignity and Confidentiality Policy and Procedure and Agreement Form

- Individual Values and Beliefs Policy and Procedure
- Violence, Abuse, Neglect, Exploitation and Discrimination policy

References

- Australian Privacy Principles (APPs) set out in the Privacy Act 1988 (Cwlth) amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cwlth)
- Health Records Act 2001 (Vic)
- Information Privacy Act (2000) (Vic)
- Freedom of Information Act 1982 (Cwlth).
- Good Practice Guideline Privacy, intake and consent in private practice <https://pacfa.org.au>
- National Disability Insurance Scheme Act 2013
- NSW - Privacy and Personal Information Protection Act 1998 No 133
- NSW - Health Records and Information Privacy Act 2002 No 71.
- Office of the Victorian Information Commissioner
- Privacy Policy, Department of Human Services, endorsed June 2002 (amended August 2005) (Vic)
- Practice Standards and Quality Indicators 2021
- United Nations Convention on the Rights of Persons with Disabilities 2018
-

Note

- (1) Halaxy is a practice management software that provides extensive features for health practitioners.
- (2) Security: Halaxy ensures bank-grade security with 256-bit encryption for data protection.

Approved By: InSyncCS Director		Version: 1.01		Created by: Jennifer Manwaring	
Approval Date	Jan 2020	Implementation Date	Aug 2024	Review Date	Aug 2027



Confidentiality Agreement

To be completed by Director, Staff, and Contractors

.....

(Name)

(Position)

has been provided with information about the-:

- Privacy and Personal Information Protection Act 1998 No 133
- Health Records and Information Privacy Act 2002 No 71
- And InSyncCS Confidentiality Policies and Procedures.

- i. I fully understand that I am required to operate within the guidelines set out in these documents listed above.
- ii. I will ensure that I confidentially maintain the health and personal information of InSyncCS clients, staff, contractors, community members, consultants, and other individuals, in all aspects of my work with InSyncCS.
- iii. I will not share any such health or personal information with any other person, without the consent of the clients, staff, contractors, community members, consultants, and other individuals (or Director in urgent cases).
- iv. I understand that to breach (break) the confidentiality of others, during the course of my position with InSyncCS, would be considered serious misconduct, and will be dealt with appropriately by the Director.

Signed:

Date:

Witness Signature:

Date:

References

- NDIS Act 2013
- Disability Act 2006
- Privacy Act 1988
- Information Privacy Act 2000
- Health Records Act 2001
- Charter of Human Rights and Responsibilities.

Approved By: InSyncCS Director		Version: 1.01		Created by: Jennifer Manwaring	
Approval Date	Jan 2020	Implementation Date	Aug 2024	Review Date	Aug 2027