Privacy and confidentiality

Version: 1
Published: -
Last edited: 10 Jun 2020, 3:52 PM
Approved: 10 Jun 2020, Robyn Torney
Next review: 1 Jun 2021

Outcome

Each participant accesses supports that respect and protect their dignity and right to privacy.

Introduction

Phoenix Lifestyle Support Association Incorporated (PLSA Inc) will ensure we protect and handle personal information in accordance with the NDIS and relevant privacy legislation. We acknowledge an individual's right to privacy while recognising that personal information is required to be collected, maintained and administered in order to provide a safe working environment and a high standard of quality. Information will only be disclosed with permission and will adhere to legislative requirements.

The information we collect is used to provide services to participants in a safe and healthy environment with individual requirements, to meet duty of care obligations, to initiate appropriate referrals, and to conduct business activities to support those services.

Applicability

When
• applies to all personal information and sensitive personal information including the personal information of employees and participants • applies to all company confidential information - that is any information not publicly available.

Who
• applies to all representatives of PLSA Inc including management, management committee members, employees, contractors and volunteers.

Definitions

Term	Description

data breach	A data breach is type of security incident where personal, sensitive or confidential information normally protected, is deliberately or mistakenly copied, sent, viewed, stolen or used by an unauthorised person or parties. A data breach where people are at risk of serious harm as a result, is reportable to the Office of the Australian Information Commissioner.
personal information	Personal information includes (regardless of its accuracy): • name • address • phone number • email address • date of birth • recorded opinions or notes about someone • any other information that could be used to identify someone.
sensitive personal information	Sensitive personal information can include personal information that is normally private such as: • health information • ethnicity • political opinions • membership of a political association, professional or trade association or trade union • religious beliefs or affiliations • philosophical beliefs • sexuality • criminal record • biometric information (such as finger prints).

Other references:

- Australian Privacy Principles 2014

Documents relevant to this policy

- CM1.3.1 Consent for Information Release
- CM1.3.2 Permission to Photograph
- CM1.3.3 Privacy Information Agreement
- CM2.4.1Confidentiality Agreement For Committee Members
- CM2.4.2 Confidentiality Agreement Employee
- Disability Services Act 2006 (Qld)
- Information Privacy Act 2009 (Qld) (legislation)
- NDIS (Provider Registration and Practice Standards) Rules 2018 (Cth)
- NDIS (Quality Indicators) Guidelines 2018 (Cth)
- Privacy Act 1988 (Cth)
- Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) (legislation)
- Privacy Regulation 2013 (Cth)
- Public Records Act 2002 (Qld)

Privacy and confidentiality guidelines

- We are committed to complying with the privacy requirements of the Privacy Act, the Australian Privacy Principles and the Privacy Amendment (Notifiable Data Breaches) Act as required by organisations providing disability services.
- We are fully committed to complying with the consent requirements of the NDIS Quality and Safeguarding Framework and relevant state or territory requirements.
- We provide all individuals with access to information about the privacy of their personal information.
- Each individual has the right to opt out of consenting to and providing their personal details if they wish.
- Individuals have the right to request access to their personal records by requesting this with their Key worker or the Manager.
- Where we are required to report to government funding bodies, information provided is non-identifiable and related to services and support hours provided, age, disability, language, and nationality.
- Personal information will only be used by us and will not be shared outside the organisation without your permission unless required by law (e.g. reporting assault, abuse, neglect, or where a court order is issued).
- Participants have the option of being involved in external NDIS audits if they wish.

Security of information

- We take reasonable steps to protect the personal information we hold against misuse, interference, loss, unauthorised access, modification and disclosure.
- Personal information is accessible to the participant and is available for use by appropriate personnel.
- Security for personal information includes password protection for IT systems, locked filing cabinets and physical access restrictions with only authorised personnel permitted access.
- Personal information no longer required is securely destroyed or de-identified, after it has been stored for the required time by legislation.

Participant record keeping

A new file (paper and electronic) will be created by the key staff/NDIS coordinator in partnership with the manager on acceptance of the participant's placement with PLSA Inc. All information is recorded on this file and is the responsibility of the key staff to keep updated.

PLSA Inc will only collect information about the participant that can be shown to be directly relevant to effective service delivery and the key staff/NDIS coordinator will:

- Seek the written consent of the participant/family/advocate prior to obtaining information from any other source CM1.3.1 Consent for Information Release
- Explain to the participant/family/advocate why the information has been requested.
- Not release any information about a participant without written permission from themselves or their legal guardian.
- Ensure only PLSA Inc employees that require it, will gain access to the above information.
- During the early stages of the referral process, advise the participant/family/advocate of:
    - PLSA Inc's policy and practices on privacy, dignity and confidentiality
    - their right to be provided with a copy of the policy, and
    - their right to view the information PLSA Inc keeps.
- Ensure that participants/family members/advocates are provided with access to an independent support person of their choice to assist them in matters relating to collection, storage, disposal and accessibility of personal information. The individual handbook provides contact details for advocacy agencies.
- Ensure that personal information about a participant is only held by PLSA Inc as long as it remains relevant to:
    - the delivery of effective services
    - PLSA Inc duty of care obligations, and
    - obligations under law.
- Promptly investigate, remedy and document any complaint or grievance regarding privacy, dignity or confidentiality, this includes an inquiry or complaint about an Australian Privacy Principle (APP). All complaints made about an APP will be reported to the management committee meeting and be managed as part of the risk management process. In addition the matter will be managed in accordance with the Complaint management policy
- Participant files are stored in lockable filing cabinets in a non-public place in the office and files are returned to their proper location as soon as they are no longer required. Electronic copies are stored on PLSA Inc's computers and password protected.
- If participant files are transported outside the organisation, or between various sites controlled by the organisation, these files are carried in a locked bag.
- No information about participants or employees will be released to recipients overseas, this includes cloud computing arrangements.
- Discuss and confirm with participants and their families at least once a year through the Satisfaction Survey (CM2.3.1 Family/Guardian SIL Satisfaction Survey or CM2.3.2 Family/Guardian Satisfaction Survey In Home Respite and Community Participation) they understand that PLSA Inc keeps their information safe and only approved people are allowed to see it.

As part of the induction process, all employees and management committee members are required to sign a confidentiality agreement (CM2.4.2 Confidentiality Agreement Employee /CM2.4.1 Confidentiality Agreement For Committee Members) and PLSA's Code of Conduct (CM2.7.8 Code of Conduct Employees/CM2.1.8 Code of Conduct for Committee Members).

When participants or employees exit the organisation, it is policy that all documentation relating to them regarding PLSA Inc's support and services be archived for the required term under legislation and then destroyed.

Staff record keeping

All staff records are kept in the main office and only the manager and authorised employees have access to these records. These are kept in filing cabinet under lock and key. Staff can access their records at any time by requesting this with the manager who will organise it. Files are to be read in the PLSA Inc office and are not to be taken off the premise.

Electronic records

All electronic records are password protected and only the manager, management committee, treasurer and appropriate employees have access to the password.

Photographic, video or other identifying images are not displayed or aired publicly without the written prior permission of the participant/family member or advocate.

Notifiable data breaches

- We will take reasonable steps to reduce the likelihood of a data breach occurring including storing personal information securely and accessible only by relevant staff.
- If we know or suspect personal information of a participant and family has been accessed by unauthorised parties, and we think this could cause harm, we will take reasonable steps to reduce the chance of harm and advise participant/family of the breach. This notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner (Commissioner) must also be notified of eligible data breaches.

Breach of privacy and confidentiality

- A breach of privacy and confidentiality is an incident—follow the Manage incident internally process to resolve.
- A breach of privacy and confidentiality may require an investigation.
- An intentional breach of privacy and confidentiality will result in disciplinary action up to and including termination of employment.

Roles and responsibilities

The manager is responsible for ensuring compliance with this policy. All employees are responsible for implementing the requirements of this policy.