PRIVACY AND CONFIDENTIALITY POLICY

PRIVACY AND CONFIDENTIALITY OF INFORMATION

GM 07

Authorised By: Chief Executive Officer	Date Effective: January 2017
Review / Consultation: Senior Managers	Review Date: January 2019

PURPOSE AND SCOPE:

The purpose of this policy is to ensure:

- the right to privacy, dignity, and confidentiality is recognised and respected always in accordance with individual needs and preferences
- personal or sensitive information is collected, held, used, and disclosed in accordance with the Australian Privacy Principles (APPs) and the NSW Health Privacy Principles (HPPs).
- methods for managing personal, sensitive and health information are open and transparent manner
- personal information and health information of Clients/ Representatives, clients, staff, (paid, voluntary, contractors and visiting health professionals)
- information is collected for relevant purposes only
- access to and correction of personal information is regulated

The policy applies to all persons involved in our organisation. This includes Clients/ Representatives, their nominated representative, clients, prospective candidates for employment, employees and any person who provides us with their personal information.

PRIVACY OFFICER

Information about the operational aspects of this policy can be obtained from our Privacy Officer.

Our Privacy Officer:	Operations Manager
Address:	Level 1, 22 Horwood Place, Parramatta NSW 2150
	(Greenway Plaza Office Suites)
Telephone:	1300 799 941
Email:	info@osanability.com.au

GENERAL PRINCIPLES

- All information relating to Clients/ Representatives, and Staff will be treated confidentially
- Generally, personal information will not be released to another person without consent.
- Clients/ Representatives have the right to access their own medical records in the presence the Care Manager or HC Manager following a written request.
- Resident's mail is not to be opened or read by staff unless the Resident/ Client/ Representative requests or requires assistance.
- Staff are to seek permission from Clients/ Representatives before entering their room or private areas.
- Privacy must be given to each Resident/ Client/ Representative when undertaking personal activities e.g. bathing, toileting, dressing, and personal/intimate relationships.
- Clients/ Representatives are to be allowed privacy when speaking with visitors and during phone conversations.
- A Resident/ Client/ Representative's personal property is their own and staff and other Clients/ Representatives are not free to use it unless invited to do so.
- The environment within the facility is to be free from undue noise. Clients/ Representatives may be asked to use earphones if their sound equipment is too loud.
- Clients/ Representatives are to be addressed by their preferred name.

DEFINITIONS

Personal information is defined as any information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Sensitive information is a subset of personal information and is information about an individual's:

- Racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; or criminal record
- Health information about an individual
- Genetic information (that is not otherwise health information)
- Biometric information that is to be used for automated biometric verification or biometric identification
- Biometric templates.

PERSONAL INFORMATION

Osan Ability Assist (OAA) collects and holds the personal information of Clients/ Representatives, employees, volunteers, and contractors. The personal information we may hold includes the following:

Clients/ Representatives

- Name
- Date of Birth
- Country of Birth and whether you are of Aboriginal and/or Torres Strait Islander origin
- Current address
- Next of Kin details
- Person responsible for Resident/ Client/ Representative, e.g. Power of Attorney, Enduring Power of Attorney, Guardian, Trustee, etc.
- Entitlement details including Medicare, Pension and health care fund
- Medical history
- Family medical history
- Social history
- Religion
- Clinical information including assessments and monitoring charts
- Care Plans
- Progress Notes
- Pathology results
- X-ray results
- Commonwealth ACFI information
- Financial and Billing information including Income and Asset Notifications
- Accident and incident forms
- Medication Charts
- Aged Care Assessment Team Referral Form (ACCR) and NSAF
- Residency Agreements
- Nursing, medical and allied health information
- Photographs (for medical purposes such as medication administration).

Employees

- Name
- Date of Birth / Country of Birth

- Address and contact details
- Details of Next of Kin
- Occupation
- Employment history
- Employment Application Form
- Citizenship, Passport and/or Visa permit
- Medical history or fitness for work information
- Immunisation records
- Employment References
- Tax File Number
- Bank Account Details
- HR/Personnel Records including Superannuation Fund
- National Police Certificate (Criminal History Record Check)
- Workers compensation or injury information
- Qualifications, Training, and Competency records.

Volunteers

- Name
- Date of Birth / Country of Birth
- Address and contact details
- Details of Next of Kin
- National Police Certificate (Criminal History Record Check)
- Drivers licence if relevant.

Contractors

- Name
- Address and contact details
- Qualifications, licenses, etc.
- Contractor Agreement
- Insurances including Workers Compensation, Professional and Public Liability
- National Police Certificate (Criminal History Record Check).

COLLECTION AND USE OF PERSONAL INFORMATION

Generally, we will only collect personal information if it is necessary to provide health services and to comply with our obligations under Australian law (e.g. tax office obligations, immigration legislation, industrial instruments, etc.), or a court/tribunal order.

In most cases, we will only collect information directly from the individual with their consent.

Personal information may be gathered from forms, telephone calls, faxes, e-mails, face to face meetings, interviews, and assessments.

Where information is collected from other sources, we will inform the individual that we hold their personal information.

Unsolicited personal information and information that is no longer required for the delivery of health services will be destroyed or de-identified as soon as practicable if it is lawful and reasonable to do so.
The potential consequences of not allowing us to collect and hold the required personal information are that we may be unable to:

- Provide appropriate health care and health services and meet our legislated obligations
- Meet the individual requirements of the care recipient
- Provide continuing employment to an employee
- Continue with the services of a contractor or volunteer.

If we receive unsolicited information such as personal information that is not relevant to the functions of the organisation, we will de-identify or destroy the information as soon as practicable.

OAA may use camera surveillance systems (CCTV) to maintain the safety and security of Clients/ Representatives, staff, visitors and other attendees. We will comply with the APPs and this Privacy Policy in respect of any personal information collected via CCTV.

When you use our website, we do not attempt to identify you as an individual user and we will not collect personal information about you unless you specifically provide this to us (e.g. through an online form).
When you use our website, our Internet Service Provider (ISP) will record and log for statistical purposes the following information about your visit:

- your computer address

- your top-level name (e.g. .com, .gov, .org, .au etc.);
- the date and time of your visit
- the pages and documents you access during your visit
- the browser you are using.

Our web-site management agent may use statistical data collected by our ISP to evaluate the effectiveness of our web-site. We are obliged to allow law enforcement agencies and other government agencies with relevant legal authority to inspect our ISP logs, if an investigation warrants such inspection.

Our website uses temporary 'cookies' to identify and interact more effectively with your computer. A 'cookie' is a small text file placed on your computer by the web server when you access our website. Our use of temporary cookies means that when you close your browser no personal information is retained that may identify you in the future.

We may create links to third party websites. OAA is not responsible for the content or privacy practices employed by websites that are linked from our website.

DISCLOSURE OF PERSONAL INFORMATION

Personal information will generally only be disclosed by authorised persons.

Personal information may be disclosed if we:

- are required or authorised by Australian law or a court/tribunal order
- reasonably believe that the disclosure is necessary to lessen or prevent a serious or imminent threat to an individual's life, health or safety, or a serious threat to public health or safety
- have reason to believe that an unlawful activity has been, is being, or may be engaged in.

Personal information may be disclosed to other persons as part of the provision of health services, including:

- Other health care professionals that are or may be involved in the care of Clients/ Representatives or employees including general practitioners, hospitals, and other allied health providers
- Other external agencies that we have contracts with to provide services to Clients/ Representatives and employees on our behalf. In circumstances where this is necessary, these external agencies are required to provide confirmation of their compliance with the Privacy Act 1988 (Cth)

- Funding bodies and other government agencies as required by Commonwealth and State legislation
- The person designated by the Resident/ Client/ Representative as the person responsible for giving and accessing their information.

We will not include personal and health information about an individual in a computerised system that is designed to link health records held by different organisations.

If it is necessary to transfer personal information to someone interstate or overseas, we will comply with this policy and the APPs, and take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information.

Personal information relating to Clients/ Representatives and employees will not be used for other purposes such as fundraising or direct marketing activities without seeking written consent of the person or the person responsible for the Resident/ Client/ Representative.

No unauthorised statements will be made regarding OAA, its Clients/ Representatives, or staff to any media representatives.

SECURITY OF PERSONAL INFORMATION

We will take all reasonable steps to protect the personal information we hold from misuse and loss, and from unauthorised access, modification, or disclosure.

We will hold all personal information in a secure and confidential manner and take all reasonable steps to ensure personal information is secure (e.g. All computers have password access, and personal information is kept in secure areas).

All our electronic systems that hold personal information have up to date security protection systems and are reviewed on a regular basis and tested to ensure they are efficient and able to meet any potential interference that might occur.

We will train all staff with access to personal information about their obligations concerning confidentiality of personal information and the privacy of individuals.

We will ensure secure disposal of electronic and paper based records.

In the event of loss of personal information, we will:

- seek to identify and secure the breach to prevent further breaches

- assess the nature and severity of the breach
- commence an internal investigation in relation to the breach.
- report the breach to police where criminal activity is suspected
- notify the Privacy Commissioner if the breach is significant
- inform the affected individual(s) where appropriate and possible.

OAA may enter into arrangements with third parties to store data we collect, including personal information, outside of Australia. We will take reasonable steps to ensure that the third party is bound by privacy protection obligations which are the same (or substantially the same) as the APPs. OAA will require any third party to have information security measures approved by us.

ACCESS TO PERSONAL INFORMATION

We will take all reasonable steps to provide access to the personal information that we hold within a reasonable period of time in accordance with the APPs.

Requests for access to the personal information we hold should be made in writing to our Privacy Officer using the **Request for Access to Personal Information** form.

Please note that OAA may recover reasonable costs associated with supplying this information to you.

We may not provide access to the personal information we hold about an individual when:

- release of the personal information would be unlawful
- the information may be subject to legal proceedings
- release of the personal information would pose a serious threat to the life, health, or safety of an individual or to public health or public safety
- release is likely to have an unreasonable impact upon the privacy of other individuals
- the information could compromise our business operations
- the request is assessed as vexatious or frivolous.

We will provide reasons for denying or refusing access to personal information in writing. This correspondence will include information concerning the mechanisms for lodging a complaint.

QUALITY AND CORRECTION OF PERSONAL INFORMATION

We will take all reasonable steps to ensure that the personal information we collect, use, hold, or disclose is accurate, complete, and up to date.

Individuals may request that personal information we hold is corrected if it is inaccurate, out of date, incomplete, irrelevant, or misleading.

We will take all reasonable steps to correct the personal information we hold.

We will provide reasons for not complying with requests to correct personal information in writing.

USE OF GOVERNMENT ISSUED IDENTIFIERS

We will not use government issued identifiers (a number assigned by a government agency to an individual as a unique identifier) for our operations.

We will not use or disclose a government issue identifier assigned unless the disclosure is necessary to fulfil our organisational obligations or is required under an Australian law or a court/tribunal order.

ANONYMITY

We will provide individuals the option of not identifying themselves, or of using a pseudonym, where it is lawful and practicable to do so.

Requests for anonymity or use of a pseudonym must be made in writing to the Privacy Officer.

BREACHES OF PRIVACY

Where a person believes that a breach of this policy or the Privacy Act has occurred, a written complaint should be made to our Privacy Officer.

All complaints will be dealt with confidentially and promptly in accordance with our internal processes (Refer to Standard 3.2 Regulatory Compliance).

Where possible, complaints should be made within six months from the time the complainant became aware of the alleged breach.

All complainants will be provided with a written response to their complaint/s in a timely manner. This response will outline the outcome of the investigation; what action is proposed to prevent such complaints being raised in the future; together with information as to how the complainant

can lodge a complaint with appropriate third party external organisations if the outcome of the investigation is considered unsatisfactory by the complainant.

If the outcome of the investigation indicates a breach of the Privacy Act has been committed, the Privacy Officer will contact the Privacy Commissioner regarding the finding and the corrective actions instituted.

If you do not receive a response from our Privacy Officer within 30 days, or you are dissatisfied with the response, you may complain to the Office of the Australian Information Commissioner (OAIC) through:

- the online Privacy Complaint form
- by mail: GPO Box 5218, Sydney NSW 2001
- by fax: +61 2 9284 9666
- by e-mail: enquiries@oaic.gov.au (note: email that is not encrypted can be copied or tracked).

FURTHER INFORMATION

Additional general information about privacy rights and privacy law is available from the Office of the Australian Information Commissioner by:

- calling their Privacy Hotline on 1300 363 992
- visiting their web site at http://www.oaic.gov.au/
- writing to:

  The Australian Information Commissioner
  GPO Box 5218
  Sydney NSW 1042

REFERENCES

- Aged Care Act 1997
- Australian Privacy Principles 2014
- Privacy Act 1988
- Privacy Amendment (Enhancing Privacy Protection) Act 2012
- Health Records and Information Privacy Act 2002 (NSW).
- Charter of Rights and Responsibilities for Home Care
- Work Health and Safety Act (2011) No 10
- Community Packaged Care Guidelines (2011)
- Ten Steps to Protecting Other People's Privacy Booklet
- Disability Standards 2013
- NSW Disability Inclusion Act and Regulation 2014

RELATED DOCUMENTS

- Privacy Agreement - Staff
- Privacy Consent – Resident/ Client
- Subcontractor Privacy Agreement
- Privacy Register