S. ANTONIO DA PADOVA NURSING HOME

PRIVACY
POLICY AND PROCEDURES

POLICY AND PURPOSE

- To ensure (Organisation) acts in a serious and committed manner to meet obligations under the Privacy Act ensuring personal or sensitive information is collected, held, used, and disclosed in accordance with the Australian Privacy Principles (APP).
- To comply with our obligations under the Australian Privacy Principles (APP), as set out in the *Privacy Act 1988* (Cth) and the *Privacy Amendment (enhancing Privacy Protection) Act 2012* (Cth).
- To ensure all legislated notifiable breaches are identified, investigated and communicated as per legislative requirements of The Privacy Amendment (Notifiable Data Breaches) Act 2017
- To support the privacy and confidentiality rights of residents, staff and visitors to the Home by meeting the requirements of the Surveillance Devices Act 2007.

KEY 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 defined as information or an opinion (that is also personal 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 the purpose of automated biometric verification or biometric identification
    - biometric templates.

- **Notifiable data breach –** where there has been unauthorised access or disclosure of personal information it holds, or such information has been lost in circumstances where that's likely to lead to unauthorised access or disclosure; and a reasonable person would conclude that such access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates.

- **Surveillance device** - means a data surveillance device, a listening device, an optical surveillance device, or a tracking device.

- **Listening device** - means any device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment.

- **Optical surveillance device** - any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment

- **Tracking device** - any electronic device capable of being used to determine or monitor the geographical location of a person or an object.

PROCEDURE

Personal information
(Organisation) collects and holds the personal information of customers, employees, volunteers, and contractors. 'Personal information' means information we hold about you from which your identity is either clear or can be reasonably determined. The personal information we may hold includes the following:

Customers
- 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 customer, 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 records entered on the 'My Aged Care' system
- Resident 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

- 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, emails, face to face meetings, interviews and assessments.
- 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.
- 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”.

Disclosure of personal information

- 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 customers or employees including general practitioners, hospitals, and other allied health providers
    - Other external agencies that we have contracts with to provide services to customers 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 customer as the "person responsible" for giving and accessing their information
- If it is necessary to transfer personal information to someone 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 customers 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 customer.

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 of our electronic systems that hold personal information have up to date security protection systems. These 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 Office of the Australian Information Commissioner if the data breach is likely to cause serious harm under the Notifiable Data Breaches scheme
    - inform the affected individual(s) where appropriate and possible so that individuals have the opportunity to take steps to protect their personal information after a data breach.

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 Australian Privacy Principles.
- Requests for access to the personal information we hold should be made in writing to the Director of Nursing.
- 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.

Surveillance

- Any devices in use will be supplied by the service. Personal devices will not be used for surveillance
- Any surveillance material stored electronically will be archived and destroyed as per policy
- Listening devices will not be used at our service other than to record a conversation or meeting to which all parties consent, expressly or impliedly, to the listening device being used. Permission to use the device must be documented at the commencement of the meeting and stored with minutes of the meeting.
- Optical surveillance devices –
    - Cameras will only be used with the consent of resident or staff member. The camera will be a device supplied by the (Organisation). Personal cameras are not to be used under any circumstances. Examples of approved camera use may include: recording of clinical progress, e.g. wound healing or recording of social events for publishing in a newsletter
    - CCTV is installed at the service and signage is installed on all external doors to advise all visitors to the service of the use of this device. CCTV is installed in common areas only excluding bathrooms and changerooms.

- Tracking devices – tracking devices such as alert bands or anklets will only be used with the consent of the resident or their legal Guardian. Management will discuss the use of this device with the resident or Guardian and will record this conversation in progress notes and in the care plan.

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 use or disclosure is necessary to fulfil our organisational obligations (such as tax file numbers for employees) 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.

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 the Privacy Officer, (designated position within the organisation). All complaints will be dealt with confidentially and promptly.

1. Notification

- Customers, families, friends or staff who have complaints about how we have dealt with personal information may apply for an internal review.
- Applications for an internal review may concern conduct a person believes is:
    - A Breach in information protection procedure
    - A breach in the code
    - An inappropriate disclosure by us of personal information
    - Application for the internal review should be made in writing to the Privacy Officer. This application should be made within six months from the time the applicant became aware of the alleged breach or inappropriate disclosure.

2. Nomination of Internal review team

- In receiving an application and conducting an internal review under the Privacy Act, we will nominate an investigation team within two weeks of receiving the compliant by the Privacy Officer.

Conducting the Privacy Review

- The internal review team will take the following steps in conducting the review:
    - Assist the applicant as much as possible
    - Interview relevant staff, examine records and obtain any other pertinent information on the circumstances of the alleged breach.
    - Seek advice from court and legal service or from Office of the Australian Information Commissioner as required.
    - Determine whether a breach of the Privacy Act has occurred and, if so, what harm or damage it has caused to the applicant.
    - Prepare a report and submit the finalised investigation report to the Privacy Officer setting out the relevant facts, the conclusions reached and recommendations for action to be taken to resolve the complaint.
    - If the outcome indicates a breach of the Privacy Act has been committed, the Privacy Officer will contact the Australian Information Commissioner regarding the finding and the corrective actions instituted.
    - The Privacy Officer will indicate outcomes to the applicants and ensure that they are aware of the Office of the Australian Information Commissioner who can investigate privacy complaints from individuals about private sector organisations and government agencies.

Completion of Internal review

- Once an application for an internal review is received, the review will be completed as soon as reasonably practicable.
- If the review is not conducted with 60 days, the applicant can seek a review by the Privacy Officer.
- Once the review is completed, the Privacy Officer may decide to:
  - Take no further action on the matter
  - Recommend a formal apology to the applicant
  - Take appropriate remedial action
  - Provide an understanding that the conduct will not occur again
  - Implement measures to prevent recurrence of the conduct.

Contacting the Privacy Officer

Contact Details: privacy@s-antonio-da-padova.com
Phone: 0298092211

All stakeholders are encouraged to contact the Privacy Officer in relation to any privacy concerns or breaches.

Further information
Additional information about the operational aspects of this policy can be obtained from our Privacy Officer.

You can obtain further general information about your privacy rights and privacy law from the Office of the Australian Information Commissioner by:

- calling their Privacy Hotline on 1300 363 992
- visiting their web site at www.oaic.gov.au
- emailing: enquiries@oaic.gov.au
- writing to:
  The Office of the Australian Information Commissioner
  GPO Box 5218
  Sydney NSW 2001

RELATED DOCUMENTS

- Privacy Agreement Customer
- Privacy Register
- Staff Confidentiality Agreement
- Information Technology and Communication Agreement
- Request for Access to Personal Information Form
- Breach of Privacy Investigation Form

RELEVANT LEGISLATION

- Aged Care Act 1997 (Cth)
- Australian Privacy Principles 2014
- Privacy Act 1988 (Cth)
- Privacy Amendment (enhancing Privacy Protection) Act 2012 (Cth)
- Relevant State & Territory Privacy Acts
- The Privacy Amendment (Notifiable Data Breaches) Act 2017
- Surveillance Devices Act 2007 (NSW)

S. Antonio da Padova
Nursing Home