Juliana Village Association Ltd

POLICY - PRIVACY AND CONFIDENTIALITY POL/GM3		
Authorised by: General Manager	Authorised on: February 2017	No of Pages: 7

Policy Statement

Juliana Village takes its obligations under the Privacy Act seriously and is committed to ensuring that personal or sensitive information is collected, held, used, and disclosed in accordance with the Australian Privacy Principles (APP) and Privacy Amendment (Notifiable Data Breaches) Act 2017.

'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 the purpose of automated biometric verification or biometric identification
- biometric templates.

Privacy Officer

Our Privacy officer is:

Name	Julie Farquhar
Position	General Manager
Contact Details	02 9541 3400

Purpose

To comply with our obligations under the Australian Privacy Principles (APP), as set out in the *Privacy Act 1988* (Cth), *Privacy Amendment (enhancing Privacy Protection) Act 2012* (Cth) and the Privacy Amendment (Notifiable Data Breaches) Act 2017.

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

Relevant Legislation

Aged Care Act 1997 (Cth)

Australian Privacy Principles 2014

Privacy Act 1988 (Cth)

Privacy Amendment (enhancing Privacy Protection) Act 2012 (Cth)

Privacy Amendment (Notifiable Data Breaches) Act 2017

Relevant State & Territory Privacy Acts including:

- *Privacy and Personal Information Protection Act 1998* (NSW)
- *The Health Records and Information Privacy Act 2002* (NSW)
- *The Guide to Aged Care Law - 2014*

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 http://www.oaic.gov.au/
- writing to:

  The Australian Information Commissioner

  GPO Box 5218

  Sydney NSW 1042

Personal information

Juliana Village collects and holds the personal information of residents, 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:

Residents

- 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, 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)
- 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 (including APRAH), Training and Competency records
- Photographs of staff on Time Target

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 residents or employees including general practitioners, hospitals, and other allied health providers
    - Other external agencies that we have contracts with to provide services to residents 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 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 residents 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.

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 Privacy Commissioner if the breach is significant
    - inform the affected individual(s) where appropriate and possible.

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 General Manager.
- 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 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.

Breaches of Privacy/Notifiable Data Breaches

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). All complaints will be dealt with confidentially and promptly.

Where individual/s are likely at risk of serious harm as a result of a data breach the individual/s will be notified by the Privacy Officer and the matter reported to the Australian Information Commissioner.

1. Notification

Residents or relatives 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:

- Breaches in information protection procedure
- Breaches in the code
- 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 6 months from the time the applicant became aware of the alleged infringing of conduct
- In the event of a notifiable data breach, the Privacy Officer will publicise the issue, with the intention of bringing it to the attention of others who might be affected. Others include staff, residents, resident representatives and contractors.

2. Nomination of Internal review team

In receiving an application or becoming aware of a notifiable data breach and conducting an internal review under the PPIP Act, we will nominate an investigation team within 24 hours.

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 Privacy Council as required.
- Determine whether a breach of the PPIP 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 Privacy 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 right of appeal to the Administrative Decisions Tribunal.

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.

Related Policies

- Pol/RM7 - Documentation
- Pol/GM1 - Governance
- Pol/GM7 - Information Technology

Related Flow Charts

- FC 3 - Document Control