Anthem Care for life	**PRIVACY**	**POLICY & PROCEDURE** **Date:** June 2019 **Review:** June 2022

Contents

Anthem Care for life	**PRIVACY**	**POLICY & PROCEDURE** **Date:** June 2019 **Review:** June 2022

AUTHORISATION

Authorised by: Chief Executive Officer

Review/Consultation: Residents / representatives and Senior Managers

DISTRIBUTION: Residents / representatives, staff, volunteers

RISK: High

POLICY

- To ensure Anthem 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) and the Aged Care Quality Standards.
- To comply with the 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 is respected
- To ensure all residents, staff and visitors are informed of and understand the surveillance mechanisms in place and the requirements of the *Surveillance Devices Act 2007* are met at the Home.

KEY DEFINITIONS

Personal information	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	A data surveillance device, a listening device, an optical surveillance device, or a tracking device.
Listening device	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.
Safety device (tracking)	Any electronic device capable of being used to determine or monitor the geographical location of a person or an object.

PROCEDURES

Responsibilities

- The FM is responsible to ensure there is a system at the Home that meets legislated privacy requirements for all stakeholders. This includes an effective system that manages and safeguards the following in relation to personal information:
    - Information provision and consent
    - Appropriate collection
    - Storage
    - Distribution
- The FM and CM must ensure there is a system to safeguard the personal privacy of all residents, including maintaining privacy in the delivery of care and clinical care.
- All staff, contractors, volunteers and visitors are responsible for ensuring the privacy of staff, contractors, volunteers and visitors is safeguarded in accordance with their training and role responsibilities. This includes the obligation to report any breaches of privacy to their Supervisor or Privacy Officer immediately.

Personal Information

The FM will ensure the Anthem collects and holds the personal information of residents, employees, volunteers and contractors. 'Personal information' means information Anthem hold about you from which your identity is either clear or can be reasonably determined. The personal information Anthem may hold includes the following:

- Residents
    - Name
    - Date of birth
    - Country of birth and whether 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 and service 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
  - Professional registrations, if relevant

- Contractors
  - Name
  - Address and contact details
  - Qualifications, registrations, licenses, etc.
  - Contractor Agreement
  - Insurances including workers compensation, professional and public liability
  - National Police Certificate (Criminal History Record Check)

Information Provision and Training

The FM must ensure:

- Residents and representatives receive information relating to privacy rights and responsibilities on admission, during orientation and ongoing via care conference, resident meetings, newsletters and any other means. This includes residents and representatives being informed of their obligation to respect the privacy of others living and working at the Home and the ways they can meet these obligations.
- Staff and contractors receive privacy training at orientation and ongoing, specifically in respect to:
  - Maintaining legal and regulatory requirements
  - Protection of any personal records in use at the Home
  - Maintaining privacy in the delivery of personal care (as applicable to role)
  - Communicating in a way that maintains privacy.
- Refer also to Dignity Policy and Procedures: Resident personal privacy in the delivery of care.

Consent

The FM must ensure:

- Resident consent to privacy arrangements is obtained on admission to the Home via the Resident Privacy Agreement.
- Resident consent is reviewed every 12 months in line with the annual case conference process. Where the resident is unable to provide written consent but has capacity to consent, the Privacy Agreement will be completed in accordance with the residents wishes by the CM or RN and a file note will be placed on the form reflecting the date, record of communication and consent and the name and designation of the person obtaining consent.
- A Privacy and Confidentiality Agreement for staff and volunteers is made upon employment and engagement, respectively.
- A Privacy Register is in operation that records the wishes of residents where they *do not* agree with any of the privacy options on the Resident Privacy Agreement. This register must be maintained as current by the Lifestyle Coordinator, with oversight

by the Director of Care, and must be available to any staff who are collecting and releasing resident's personal information.

- Where there is a specific request from the resident or representative to release information to a third party (other than those indicated in the Collection and Use of Personal Information), consent is obtained from the resident or representative in writing through the completion of a Privacy Consent Form – External Services.
- There is a system and appropriate support for resident's to withdraw or alter their privacy consent at any time.

Collection and Use of Personal Information

The FM will be responsible to ensure:

- In most cases Anthem information is collected 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, only personal information is collected 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, Anthem will inform the individual that Anthem 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 Anthem may be unable to:
    - Provide appropriate health care and health services and meet our legislated obligations.
    - Meet the individual requirements of the resident.
    - Provide continuing employment to an employee.
    - Continue with the services of a contractor or volunteer.
- If Anthem receives 'unsolicited information' such as personal information that is not relevant to the functions of the organisation, it will 'de-identify or destroy the information as soon as practicable'.

Disclosure of Personal Information

The FM will be responsible to ensure:

- Personal information may be disclosed if Anthem:
  - Is required or authorised by Australian law or a court/tribunal order.
  - Reasonably believes 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.
  - Has 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 Anthem 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.
  - Approval to disclose information by the resident or 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, Anthem 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 any group or individual 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.
- Residents, representatives and visitors must also maintain the privacy of other residents living in the home. The Resident Privacy Agreement specifically outlines this requirement. Signage and staff protocols in the home will also reinforce this requirement, for e.g. not providing information to a resident or a (visitor) without resident consent.

Security of Personal Information

The FM will be responsible to ensure:

- Anthem takes all reasonable steps to protect the personal information Anthem holds from misuse and loss, and from unauthorised access, modification or disclosure.
- All personal information is held in a secure and confidential manner and reasonable steps are taken to ensure personal information is secure (e.g. all computers have password access, and personal information is kept in secure areas).
- All 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.
- Anthem will ensure secure disposal of electronic and paper-based records.
- In the event of loss of personal information, Anthem 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

The FM will be responsible to ensure:

- All reasonable steps are taken to provide access to the personal information that Anthem holds within a reasonable period of time in accordance with the Australian Privacy Principles.
- There is communication to all stakeholders that requests for access to the personal information Anthem holds should be made in writing to the Privacy Officer.
- Anthem does not provide access to the personal information Anthem 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.

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

Surveillance

The FM will be responsible to ensure:

- Any devices in use are supplied by the Home. Staff are advised and supported to not use personal devices for surveillance. Staff are encouraged to report any matters of concern relating to the delivery of care and services to the RN in Charge or Supervisor.
- Any surveillance material stored electronically will be archived and destroyed as per the policy.
- Listening devices will not be used at the Home 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/ representative or staff member. The camera will be a device supplied by Anthem. Personal cameras are not to be used under any circumstances. Examples of approved use of camera supplied by the Home 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 change rooms or rooms with resident representative approval.
- Safety devices**,** such as alert bands or anklets to aid in monitoring a resident's location and maintain their safety 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 and services plan.
- Refer also to Work Health and Safety Policy and Procedures.

Quality and Correction of Personal Information

The FM will be responsible to ensure:

- All reasonable steps are taken to ensure that the personal information Anthem collect, use, hold, or disclose is accurate, complete and up to date.
- Individuals have the right and ability to request that personal information Anthem holds is corrected if it is inaccurate, out of date, incomplete, irrelevant or misleading.
- All reasonable steps are taken to correct the personal information Anthem held.
- Anthem provides reasons for not complying with requests to correct personal information in writing.

Use of Government Issued Identifiers

The FM will be responsible to ensure:

- 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

The FM will be responsible to ensure:

- 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.

Notification

- Residents, families, friends or staff who have complaints about how Anthem 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.

Nomination of Internal Review Team

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

Conducting the Privacy Review

- The internal investigation 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.
    - 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

- Our Privacy officer is:
  Name: Fleur Hannen
  Position: Privacy Officer
  Contact Details: 0414 588 795
- 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 Resident
- Privacy Register
- Staff Confidentiality Agreement
- Request for Access to Personal Information Form
- Privacy Consent Form – External Services

RELEVANT LEGISLATION

- Aged Care Act 1997 (Cth)
- Australian Privacy Principles 2014
- Aged Care Quality Standards 2018
- Charter of Aged Care Rights 2019
- 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)