

Privacy Policy

HO 2.16.4



Authorised by: CEO

Issued to: LT, All SC Aged Care Centres, SCHC

Preamble

This is the policy of the following entities:

- EEW Investments Pty Limited t/as SummitCare Canley Vale (ABN 60044968556)
- Wohl Investments Pty Limited t/as SummitCare Liverpool-173 and SummitCare Liverpool-155 (ABN 60002699818)
- Phillip House Nursing Home Pty Ltd t/as SummitCare Waverley (ABN 67001389626)
- Frenchmans Lodge Nursing Home Pty Ltd t/as SummitCare Randwick (ABN 54000525217)
- Stelcom Pty Limited t/as SummitCare Smithfield (ABN 85075818647)
- St. Marys Gardens Aged Care Centre Pty Ltd t/as SummitCare St Marys (ABN 13087557686)
- St. Marys Gardens Aged Care Centre Pty Ltd t/as SummitCare Penrith (ABN 54829537883)
- Stelcom Pty Limited t/as SummitCare Wallsend (ABN 85075818647)
- Hills Care Pty Ltd for Hills Care Unit Trust t/as SummitCare Baulkham Hills (ABN 40556397931)
- SummitCare HomeCare Pty Ltd t/as SummitCare At Home (ABN 99161312045)
- Summit Health Care Pty Ltd t/as SummitCare (Australia) (ABN 42003073434)
- Dontello Pty Ltd (ABN 93050335165)

collectively referred to as '**SummitCare**'.

SummitCare is bound by the 13 Australian Privacy Principles (APPs), as set out in the *Privacy Act 1988 (amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012)*.

To comply with our obligations under the APPs, SummitCare has a Privacy Policy, which sets out how we manage privacy in our organisation. Any relevant person wishing to receive more information about the operational aspects of this policy can seek that information from the Chief Executive Officer who is the Privacy Officer for SummitCare.

Purpose

To ensure that SummitCare's Privacy Policy and Procedures are clearly documented and understood by residents/clients, employees, and volunteers;

and to ensure that personal information is collected, used, stored and disclosed by SummitCare in accordance with legal requirements.

Privacy Policy



Policy Statement

SummitCare takes its obligations under the Privacy Act seriously and will take all reasonable steps in order to comply with the Act and protect the privacy of personal and sensitive information that we hold. This policy sets out how we will achieve this.

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

Relevant Legislation

Privacy Act 1988 (amended by the Privacy Amendment (Private sector) Act 2000 and the Privacy Amendment (Enhancing Privacy Protection) Act 2012)

Privacy and Personal Information Act 1988

Guardianship Act 1987

Aged Care Act 1997

Relevant Guidelines and Rules

Australian Privacy Principles Guidelines, Office of the Australian Information Commissioner

Privacy (Persons Reported as Missing) Rule 2014

Use and Disclosure of Genetic Information to a Patient's Genetic Relatives under s 95AA of the Privacy Act Guidelines

Tax File Number Guidelines 2011

SummitCare Policy Guidelines

SummitCare collects and holds the following personal information:

Employees

- Name
- Date of Birth
- Address
- Occupation
- Career history
- Application for Employment
- Immunisation records
- References

Privacy Policy



- Tax file number
- Banking details
- HR/Personnel Records
- Workers compensation or injury information
- Working with Children check
- Police check
- Immigration status report
- Garnishee orders
- Superannuation
- APRA registration
- Car registration

Residents/Clients

- Care Plans
- Progress Notes
- Pathology results
- Programme, assessment and review notes
- Morbidity information commonly referred to as “Admission Form 7 State Health”
- Commonwealth Funding Instrument information
- Financial and Billing information
- Accident and incident forms
- Medication charts
- Person responsible for resident/client e.g. Next of kin, Guardianship and Power of Attorney details
- Aged Care Client Record (ACCR)
- Residency Agreements
- Nursing, medical and allied health information

Privacy Policy



1. Collection

- SummitCare will only collect information if it is necessary for our functions and activities. When we do so, we will inform the individual about what the information will be used for. In most cases we will only collect information directly from the individual (or the responsible person, as appropriate) and where information is collected from someone else (unless required in a permitted health situation), we will inform the individual (or the responsible person, as appropriate) if practicable. If the person responsible is to be away for any reason for a certain period of time, it is the responsibility of the centre to ensure that the Consent form to collect information is signed and placed in the resident/client's file.
- Information is collected by fair and lawful means and in accordance with our obligations under State and Federal legislation in respect of residents/clients. Other information collected concerning employees is collected to ensure compliance with tax office obligations, immigration legislation and industrial instruments, and the like.
- SummitCare may collect personal and sensitive information from third parties if health information is required to provide a health service to the employee or resident/client. Where practicable, consent will be sought from the individual (or the responsible person, as appropriate) before information is sought from third parties.

2. Use and Disclosure

- SummitCare will only use or disclose personal/health care information relating to residents/clients or employees for the primary purpose of collection, a related purpose for which it was collected (and which would be reasonably expected) or a purpose to which the individual (or the responsible person, as appropriate) has consented.
- Personal and/or health care information may be provided to the following as part of provision of services:
 - Other health care professionals that are or may be involved in the care of residents/clients or employees including General Practitioners, hospitals, other allied health providers
 - Other external agencies that SummitCare contracts with to provide services to employees and residents/clients on our behalf e.g. LASA Corporate Services. In circumstances where this is necessary, these external agencies are required to provide confirmation of their compliance with the Privacy Act 1988 (*amended by the Privacy Amendment (Private sector) Act 2000 and the Privacy Amendment (Enhancing Privacy Protection) Act 2012*).
 - Funding bodies and other government agencies as required by Commonwealth and State legislation
 - The person designated by the resident/client as the "person responsible" for giving and accessing their information
 - Personal and health care information relating to residents/clients and employees will not be used for other purposes such as fundraising or

Privacy Policy



marketing activities without seeking written consent of the resident/client, person designated as the “person responsible” for the resident/client or employee

- The use or disclosure is required or authorised by law
- SummitCare reasonably believes that the use or 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
- If SummitCare has reason to believe that an unlawful activity has been, is being or may be engaged in

3. Quality of Information

SummitCare will take all reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, complete and up to date and is relevant for the purpose of the collection, use or disclosure.

4. Security of Information

- SummitCare takes all reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.
- SummitCare holds all personal information of residents/clients and employees in a secure and confidential manner.
- SummitCare destroys all personal information it no longer requires for any purpose for which the information may be used or disclosed under Part 2 of this Policy.
- Secure disposal of electronic records will include:
 - Overwriting records before they are deleted and
 - Deleting backup files
- Secure disposal of paper based records will include:
 - Shredding of paper files or
 - Contacting an authorise disposal company for secure disposal
- In situations where it is necessary to retain the personal information, it will be permanently de-identified by removing from the record any information by which a resident/client/employee may be identified.

5. Openness

- This Privacy Policy clearly expresses SummitCare’s management of personal information, and this Policy is available to any person who requests a copy.
- On written request, SummitCare will take all reasonable steps to explain generally what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

Privacy Policy



6. Access to or correction of personal information

- SummitCare provides access to the personal information that we hold about residents and employees. Access will be provided in accordance with the Australian Privacy Principles.
- A relative or family member is required to make a written request to access the personal information of a resident/client to the respective Operations Manager who will relay the request to the Privacy Officer.
- All reasonable steps will be taken to provide access.
- Requests for corrections to personal information held by SummitCare may be made in writing to the respective Operations Manager who will relay the request to the Privacy Officer.
- SummitCare will provide a reason for the denial of access or refusal to correct personal information.

6.1 Resident/Client Access

Access is granted to individuals receiving services from SummitCare and/or the person designated by the resident/client as being the “person responsible” for giving and accessing this information upon written request through the Operations Manager at the Aged Care Centre in which the resident/client resides. The “person responsible” must consider whether if able the resident/client would wish to access the information.

SummitCare is not required to provide access when:

- the request is vexatious or frivolous
- it requires access that would be unlawful
- the information would reveal SummitCare’s intention in relation to negotiations
- it concerns information related to an existing or anticipated legal proceeding
- it would detrimentally affect the privacy of another individual
- would pose a serious threat to the resident’s/client’s life or health
- the information was given in confidence

6.2 Employee Access

Access is granted to employees of SummitCare upon written request through the Operations Manager at the Aged Care Centre in which the employee is employed.

SummitCare is not required to provide access when:

- the request is vexatious or frivolous
- it requires access that would be unlawful
- the information would reveal SummitCare’s intention in relation to negotiations
- it concerns information related to an existing or anticipated legal proceeding
- it would detrimentally affect the privacy of another individual
- would pose a serious threat to the employee’s life or health
- the information was given in confidence

Privacy Policy



7. Identifiers

- SummitCare will not adopt an identifier (number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisations operations) of an individual as its own, if the identifier of the individual has been assigned by an agency, an agent of an agency or other government bodies.
- SummitCare will not use or disclose an identifier assigned to an individual by an agency as mentioned above unless the use or disclosure is necessary to fulfil organisational obligations to the agency.

8. Anonymity

SummitCare gives individuals the option of not identifying themselves where it is lawful or practicable.

9. Transborder Data Flows

In general, SummitCare does not send personal information to foreign countries. However, SummitCare may on occasion be required to transfer personal information about a resident/client, person responsible or an employee to someone who is in a foreign country if:

- SummitCare reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which upholds principles for handling the information that are substantially similar to the Australian Privacy Principles
- The individual gives informed consent
- It is not practicable for the individual to give consent, but the transfer of information is for his or her benefit
- Transfer is necessary for performance of a contract between the individual and SummitCare
- Transfer is necessary for performance of a contract between the a third party and SummitCare and is in the interests of the individual
- Action is required in relation to an unlawful activity
- Disclosure is required by law

The country to which the information is sent would depend on the individual circumstances of the case.

If it becomes necessary to store or disclose personal or sensitive information outside of Australia, where practicable an indemnity will be sought from the recipient of the information, which indemnifies SummitCare against claims for the recipient's breach of the *Privacy Act*.

Privacy Policy



10. Sensitive Information

Sensitive information refers to:

- an individual's racial or ethnic origin
- health information
- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation or practices
- criminal record
- genetic information
- biometric information that is to be used for certain purposes
- biometric templates.

SummitCare will not collect, use or disclose sensitive information about a resident/client, person responsible or employee unless:

- They have consented; or
- The collection, use or disclosure is required by law; or
- The collection, use or disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual; or
- Health information is required to provide a health service to the employee or resident/client and the collection, use or disclosure is a permitted health situation (see Part 18).

11. Complaints process

If there is a complaint regarding the information that SummitCare is collecting or has collected, or a person believes there is a breach of this policy or the Privacy Legislation, a written complaint should be made to the Operations Manager, who should refer this to SummitCare's Privacy Officer.

12. Debt Collection

SummitCare has a policy in relation to the collection of debts. Residents/clients and/or the person responsible who do not pay their fees on time may be subject to their personal information being given to a debt collection agency.

13. Direct Marketing

Personal information may be used to assist SummitCare with direct marketing, for example to enhance our service and keep relatives and stakeholders informed by sending newsletters. Individuals have the right to:

Privacy Policy



- Elect not to receive direct marketing material from us
- Direct us not to use or disclose information for purposes of direct marketing by other organisations
- Request us to provide the source of the information used for direct marketing.

14. Missing Persons

Personal information about an individual may be used or disclosed without the individual's consent to the following entities:

- the Australian Federal Police
- a police force or service of a State or Territory
- Department of Social Services
- the Salvation Army Family Tracing Service
- the Australian Red Cross Tracing Service
- International Social Service Australia
- a Link-Up Service of a State or Territory, or
- the Department of Foreign Affairs and Trade.

In the following circumstances:

- the individual has been reported as missing to one of the entities above, and
- his or her whereabouts is unknown to that entity, and
- the entity is trying to find the individual because there are serious concerns for their safety and/or welfare or for the purpose of re-uniting them with their family, and
- the use or disclosure of the information is in response to a request from one of the above entities, and
- we believe that the use or disclosure is reasonably necessary to assist the entity to locate a person reported as missing, and
- it is unreasonable or impracticable to obtain the consent of the person reported as missing to the use or disclosure of the information, and
- the information that is used or disclosed is limited to the extent reasonably necessary to make contact with, or to offer proof of life of, the person reported as missing, and
- the use or disclosure is not contrary to any wish expressed by the person reported as missing of which we are aware, and
- we do not believe that the use or disclosure would pose a serious threat to the life, health or safety of the individual.

15. Emergencies and Disasters

This part applies to situations when the Prime Minister or a Minister of the Australian government has issued a written and published declaration of an emergency or disaster of national significance and which has affected one or more Australian citizens or permanent residents (**Declaration**).

Privacy Policy



When a Declaration has been issued, we may collect, use or disclose personal information without having to comply with ordinary *Privacy Act* rules only for the following purposes:

- identifying those are or might be injured, missing, dead or involved in the emergency
- helping individuals to get services including repatriation, medical or other treatment, health, financial or other humanitarian aid
- helping law enforcement
- coordinating or managing the emergency
- making sure that people who are responsible for individuals¹ are kept appropriately informed about them and the emergency response to those individuals.

Only to the following organisations:

- a State or Territory authority
- the use or disclosure is not contrary to any wish expressed by the person reported as missing of which we are aware, and
- we do not believe that the use or disclosure would pose a serious threat to the life, health or safety of the individual
- an entity involved or likely to be involved in managing or assisting in managing the emergency or disaster, or
- a person who is 'responsible' for the individual, or
- a Minister; or
- a Department; or
- certain bodies or tribunals established or appointed for a public purpose by or under a Commonwealth enactment; or
- a body established or appointed by the Governor-General, or by a Minister, otherwise than by or under a Commonwealth enactment; or
- a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department; or
- a person holding or performing the duties of an appointment, being an appointment made by the Governor-General, or by a Minister, otherwise than under a Commonwealth enactment; or
- a federal court; or
- the Australian Federal Police; or
- Norfolk Island agency; or
- the nominated AGHS company; or
- an eligible hearing service provider; or
- the Chief Executive Officer of Medicare Australia.

Only in the following situations:

- we believe that the individual is involved in the emergency or disaster; and

Privacy Policy



- there are limits on the entities that the information can be disclosed to; and
- these entities must be directly involved in providing specific services, such as repatriation, medical, health, financial or other humanitarian assistance.

If possible, queries regarding extraordinary handling of personal and sensitive information where there has been a Declaration should be referred at first instance to the Privacy Officer.

16. Unsolicited information

If we receive unsolicited personal information, we will:

- Determine whether the information could have been collected in compliance with Part 1 of this Policy; and
- If the answer is no, then destroy or de-identify the information; or
- If the answer is yes, then provide the individual with a privacy statement and consent form and otherwise handle the information in accordance with this Policy.

17. Visitors book

- The Visitors book at reception is a tool used by SummitCare management and is not to be used or accessed by staff or residents for any purpose other than to sign visitors in and out of SummitCare facilities.

18. Permitted Health Situations

Collection – provision of a health service

A “permitted health situation” exists in relation to the collection by an organisation of health information about an individual if:

- a) the information is necessary to provide a health service to the individual; and
- b) either:
 - the collection is required or authorised by or under an Australian law (other than the Privacy Act); or
 - the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

Collection – research etc.

A “permitted health situation” exists in relation to the collection by an organisation of health information about an individual if:

- a) the collection is necessary for any of the following purposes:
 - research relevant to public health or public safety;
 - the compilation or analysis of statistics relevant to public health or public safety;
 - the management, funding or monitoring of a health service; and
- b) that purpose cannot be served by the collection of information about the individual that is de-identified information; and
- c) it is impracticable for the organisation to obtain the individual’s consent to the collection; and
- d) any of the following apply:
 - the collection is required by or under an Australian law (other than the *Privacy Act*);
 - the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation;
 - the information is collected in accordance with guidelines approved under section 95A of the purposes of this subparagraph.

Use or disclosure – research, etc.

A “permitted health situation” exists in relation to the use or disclosure by an organisation of health information about an individual if:

- a) the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety; and
- b) it is impracticable for the organisation to obtain the individual’s consent to the use or disclosure; and

- c) the use or disclosure is conducted in accordance with guidelines approved under section 95A for the purposes this paragraph; and
- d) in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information.

Use of disclosure – genetic information

A “permitted health situation” exists in relation to the use or disclosure by an organisation of genetic information about an individual (**the first individual**) if:

- a) the organisation has obtained the information in the course of providing a health service to the first individual; and
- b) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual; and
- c) the use or disclosure is conducted in accordance with guidelines approved under section 95AA; and
- d) in the case of disclosure – the recipient of the information is a genetic relative of the first individual.

Disclosure – responsible person for an individual

A “permitted health situation” exists in relation to the disclosure by an organisation of health information about an individual if:

- a) the organisation provides a health service to the individual; and
- b) the recipient of the information is a responsible person for the individual; and
- c) the individual:
 - is physically or legally incapable of giving consent to the disclosure; or
 - physically cannot communicate consent to the disclosure; and
- d) another individual (the carer) providing the health service for the organisation is satisfied that either:

Privacy Policy



- the disclosure is necessary to provide appropriate care or treatment to the individual; or
 - the disclosure is made for compassionate reasons; and
- e) the disclosure is not contrary to any wish:
- expressed by the individual before the individual became unable to give or communicate consent; and
 - of which the care is aware, or of which the carer could reasonably be expected to be aware; and
- f) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (d).

Reference Documents

HO 2.16.3 - Privacy

Revision Record

<i>Date Issued:</i>	<i>Details of changes</i>
20.09.2003	First Issue
02.11.2007	Review
12.01.2009	Reviewed and re numbered
18.05.2010	Updated to reflect corporate restructure
13.10.2010	Reviewed
28.06.2013	Amended
20.09.2013	Amended
11.03.2014	Reviewed by Kennedys
25.06.2014	Reviewed