PRIVACY GUIDELINE

1. Supporting Documentation:	Privacy Policy Media Policy Code of Conduct Policy and Guideline Privacy Collection Statement Privacy Act 2009 Freedom of Information Act 1982 Office of the Australian Information Commissioner (OAIC) website.
2. Accountability:	**Board of Directors / Chief Executive Officer** has the responsibility to ensure that this guideline is accurate and current and observed by all employees. **Senior Leadership Team relevant Chief / Manager – Regional Services / Residential Aged Care / Retirement Living / SCC Direct** has the responsibility to ensure employees are aware of this guideline. **Employees** have the responsibility to comply with Southern Cross Care Qld (SCCQ) guidelines. If unclear about the guideline, employees must seek clarification from their immediate (line) manager.
3. Scope:	This guideline applies to all employees (including contracted agency staff) and volunteers of SCCQ.
4. Approved by (signature): **Position: CFO**	Irma Hajdari

BACKGROUND/OBJECTIVE

This Guideline should be read in conjunction with Southern Cross Care (Qld) Inc.'s (**SCCQ**) Privacy Policy.

The purpose of the policy and guideline is to:

- ensure personal information is managed in an open and transparent way;
- protect the privacy of personal information, including health information, of clients and staff;
- provide for the fair collection and handling of personal information;
- ensure that personal information we collect is used and disclosed for relevant purposes only;
- regulate the access to and correction of personal information; and
- ensure the confidentiality of personal information through appropriate storage and security.
- Obligations for notifying affected individuals and Australian Information Commissioner about data breaches likely to cause serious harm.

DEFINITIONS

Personal Information is information or an opinion, whether true or not and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Sensitive Information includes information or an opinion 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, criminal record, biometric information, biometric templates, Health Information about an individual and genetic information.

Health Information is:

- information or an opinion about:
    - the health or a disability (at any time) of an individual; or
    - an individual's expressed wishes about the future provision of health services to him or her; or
    - a health service provided, or to be provided, to an individual that is also Personal Information; or
- other Personal Information collected to provide, or in providing, a health service;
- other Personal Information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances;
- genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Unsolicited Information is all Personal Information received from an individual that we did not actively seek to collect.

An **Employee Record** is a record of Personal Information relating to the employment of the employee. Examples of Personal Information relating to the employment of the employee are Health Information about the employee and Personal Information about all or any of the following:

- the engagement, training, disciplining or resignation of the employee;
- the termination of the employment of the employee;
- the terms and conditions of employment of the employee;
- the employee's personal and emergency contact details;
- the employee's performance or conduct;
- the employee's hours of employment;
- the employee's salary or wages;
- the employee's membership of a professional or trade association;
- the employee's trade union membership;
- the employee's recreation, long service, sick, personal, maternity, paternity or other leave; and
- the employee's taxation, banking or superannuation affairs.

Client Records are any information and/or item deemed to be identifiable to an individual client.

DETAILS/PROCEDURE

Collection, use and disclosure of information

We will collect and use information about you during the course of your relationship with us. We explain below how we may collect, use and disclose this information. It is important that the information we hold about you is up to date. You must let us know when the information you have provided has changed.

Purpose of collection of Personal Information

We will only collect Personal Information about an individual by fair and lawful means and only if the information is necessary for one or more of our functions as an aged care provider, home care provider and retirement village operator. Collection of the Personal Information is necessary to:

- comply with the provisions of state or commonwealth law;
- provide data to government agencies in compliance with state or commonwealth law;
- determine eligibility to entitlements provided under any state or commonwealth law;
- provide appropriate services and care;
- enable contact with a nominated person regarding a client's health status; and
- lawfully liaise with a nominated representative and to contact family if requested or needed.

Some individuals may not want to provide information to us. The information we request is relevant to providing them with the care and services they need. If the individual chooses not to provide us with some or all of the information we request, we may not be able to provide them with the care and services they require.

We will not collect your Sensitive Information (including Health Information) unless the collection of the information is reasonably necessary for or directly related to one or more of our functions and:

- you have consented to the collection of this information; or
- the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or
- a permitted general situation exists to the collection of the information;
- a permitted health situation exists in relation to the collection of the information; or
- we are a non-profit organisation and:
  - the information relates to our activities; and
  - the information relates only to the members of the organisation, or to individuals who have regular contact with us and our activities.

Methods of collection

Personal Information and Sensitive Information (including Health Information) may be collected:

- from a client;
- from any person or organisation that assesses health status or care requirements (e.g., the Aged Care Assessment Team);

- from the health practitioner of a client;
- from other health providers or facilities;
- from family members or significant persons of a client; and
- from a legal advisor of a client.

We will collect Personal Information from the client unless:

- we have the consent of the client to collect the information from someone else;
- we required or authorised by law to collect the information from someone else; or
- it is unreasonable or impractical to do so.

At admission, or upon taking possession of a retirement village unit, a client should identify any parties from whom they do not wish Personal Information accessed or to whom or which they do not wish Personal Information provided. This should be recorded in the file of the client and complied with to the extent permitted by law.

Unsolicited Information

If we receive Personal Information from an individual that we have not solicited and we could not have obtained the information by lawful means, we will destroy or de-identify the information as soon as practicable and in accordance with the law.

Staff (employee) records

We must keep a record in respect of employees about:

- basic employment details such as the name of the employer and the employee and the nature of their employment (e.g., part-time, full-time, permanent, temporary or casual);
- pay;
- overtime hours;
- averaging arrangements;
- leave entitlements;
- superannuation contributions;
- termination of employment (where applicable); and
- individual flexibility arrangements and guarantees of annual earnings.

We may also collect Personal Information about employees relating to their employment, being Employee Records (as defined above).

Notification

We will at or before the time, or as soon as practicable after we collect Personal Information from an individual take all reasonable steps to ensure that the individual is notified or made aware of:

- our identity and contact details;
- the purpose for which we are collecting Personal Information;
- the identity of other entities or persons to whom we usually disclose Personal Information;

- that our privacy policy contains information about how the individual may complain about a breach of the Australian Privacy Principles and how we will deal with a complaint;
- whether we are likely to disclose Personal Information to overseas recipients and if so, the countries in which such recipients are likely to be located and if practicable, to specify those countries.

Use and disclosure of information

Permitted disclosure

We may not use or disclose Personal Information for a purpose other than the primary purpose of collection, unless:

- the secondary purpose is related to the primary purpose (and if Sensitive Information directly related) and the individual would reasonably expect disclosure of the information for the secondary purpose;
- the individual has consented;
- the information is Health Information and the collection, use or disclosure is necessary for research, the compilation or analysis of statistics, relevant to public health or public safety, it is impractical to obtain consent, the use or disclosure is conducted within the privacy principles and guidelines and we reasonably believe that the recipient will not disclose the Health Information;
- we believe on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to an individual's life, health or safety or a serious threat to public health or public safety;
- we have reason to suspect unlawful activity and use or disclose the Personal Information as part of our investigation of the matter or in reporting our concerns to relevant persons or authorities;
- we reasonably believe that the use or disclosure is reasonably necessary to allow an enforcement body to enforce laws, protect the public revenue, prevent seriously improper conduct or prepare or conduct legal proceedings; or
- the use or disclosure is otherwise required or authorised by law.

If we receive Personal Information from an individual that we have not solicited, we will, if it is lawful and reasonable to do so, destroy or de-identify the information as soon as practicable.

Cross-border disclosure

We will not disclose an individual's Personal Information to an overseas recipient. If we do, we will take all steps that are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles, unless:

- the overseas recipient is subject to laws similar to the Australian Privacy Principles and the individual has mechanisms to take action against the overseas recipient;
- we reasonably believe the disclosure is necessary or authorised by Australian law; or
- the individual has provided express consent to the disclosure.

Disclosure of Health Information

We may disclose Health Information about an individual to a person who is responsible for the individual if:

- the individual is incapable of giving consent or communicating consent;

- the service manager is satisfied that either the disclosure is necessary to provide appropriate care or treatment or is made for compassionate reasons or is necessary for the purposes of undertaking a quality review of our services (and the disclosure is limited to the extent reasonable and necessary for this purpose); and
- the disclosure is not contrary to any wish previously expressed by the individual, of whom the service manager is aware, or of which the service manager could reasonably be expected to be aware and the disclosure is limited to the extent reasonable and necessary for providing care or treatment.

A person responsible is a parent, a child or sibling, a spouse, a relative, a member of the individual's household, a guardian, an enduring power of attorney, a person who has an intimate personal relationship with the individual, or a person nominated by the individual to be contacted in case of emergency, provided they are at least 18 years of age.

Access

You have a right to request that we provide you access to the Personal Information held about you (and we shall make all reasonable attempts to grant that access) unless providing access:

- is frivolous or vexatious;
- poses a serious threat to the life or health of any individual;
- unreasonably impacts upon the privacy of other individuals;
- jeopardises existing or anticipated legal proceedings;
- prejudices negotiations between the individual and us;
- would be unlawful or would be likely to prejudice an investigation of possible unlawful activity;
- an enforcement body performing a lawful security function asks us not to provide access; or
- giving access would reveal information we hold about a commercially sensitive decision making process.

Requesting access

Requests for access to information can be made orally or in writing and addressed to the service manager of the relevant service. We will respond to each request within a reasonable time.

Declining access

An individual's identity should be established prior to allowing access to the requested information. If unsatisfied with the individual's identity or access is requested from an unauthorised party, we can decline access to the information.

We can also decline access to information if:

- there is a serious threat to life or health of any individual;
- the privacy of others may be affected;
- the request is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings; or
- the access would be unlawful.

We will provide in writing the reasons for declining access to the requested information.

Granting access

On request (and after determining an individual's right to access the information) we should provide access to Personal Information.

Charges for access

If we charge for providing access to Personal Information, those charges will not be excessive.

Access of deceased client information

There are certain provisions in the Right to Information Act 2009 (QLD) and the Information Privacy Act 2009 (Qld) that refers to and define term 'eligible family member'. This phrase often appears in relation to information that would, if the person were alive be their personal information.

Eligible family member start at "1." and work your way through the list below.

1. A spouse married and de facto regardless of gender
2. An adult child (who is over 18 years or more)
3. A partner
4. An adult sibling
5. If none of the above persons are reasonable available
6. The next nearest adult relative who is reasonable available

If the deceased person is of Aboriginal or Torres Strait Islander community then a person who is an appropriate person according to the tradition or custom of the community to which the deceased person belongs.

Personal Information Quality

We aim to ensure that the Personal Information we hold is accurate, complete and up to date. Please contact us if any of the Personal Information you have provided to us has changed. Please also contact us if you believe that the information we have about you is not accurate, complete or up to date.

Correction

If an individual establishes the Personal Information held about them is inaccurate, incomplete, out of date, irrelevant or misleading we must take reasonable steps to correct the information.

If we disagree with an individual about whether information is accurate, complete and up to date, and the individual asks us to associate with the information a statement claiming that the information is inaccurate, incomplete, out of date, irrelevant or misleading we must take reasonable steps to do so.

If we refuse to correct the Personal Information as requested by the individual, we will give the individual written notice that sets out:

- the reasons for the refusal, except to the extent that it would be unreasonable to refuse;
- the mechanisms available to complain about the refusal; and
- any other matter prescribed by the regulations.

Direct marketing

Personal Information

We will not use or disclose Personal Information about an individual for the purposes of direct marketing, unless the information is collected directly from you and:

- you would reasonably expect us to use or disclose your Personal Information for the purpose of direct marketing; and
- we have provided you a means to 'opt out' and you have not opted out.

Sensitive Information

We will not use or disclose Sensitive Information about any individual for the purposes of direct marketing, unless the individual has consented to the information being used for direct marketing.

An individual's rights in relation to direct marketing activities

If we use information for the purposes of direct marketing the individual may:

- ask us not to provide direct marketing communications to us;
- ask us not to disclose or use the information;
- ask us to provide the source of the information.

Personal Information security

We are committed to keeping secure the Personal Information you provide to us. We will take all reasonable steps to ensure the Personal Information we hold is protected from misuse, interference, loss, unauthorised access, modification or disclosure.

Client information

- We must keep client records in secure storage.
- If the records are required to be carried for the purpose of providing care or support in the community:
  - only the employee carrying the records will have access to them; and
  - the information will be secured in storage receptacles and returned to the relevant SCCQ site when no longer required.
- Records of previous clients and earlier unused volumes of records of current clients, including electronic records, shall be archived and stored in a locked service away from general use.
- Only health professionals attending to the care of a client are to have access to information of the client. All records shall only be used for the purpose they were intended.
- A client or their representative shall be provided access to records as requested and after consultation with the service manager. At these times, a qualified employee is to remain with a client or representative to facilitate the answering of any questions raised.
- Details of clients are not to be provided over the phone, unless the employee is sure of the person making the inquiry. If in doubt, consult the service manager.

- No employee shall make any statement about the condition or treatment of a client to any person not involved in the care except to the immediate family or representative of the client and then only after consultation with the service manager.
- All employees must be discreet with their comments at all times, protecting and respecting the privacy, dignity and confidentiality of all clients.
- Handovers shall be conducted in a private and confidential manner.

Security measures

Our security measures include, but are not limited to:

- training employees about their obligations in respect to your Personal Information;
- use of passwords when accessing our data storage system;
- use of firewalls and virus scanning tools to protect against unauthorised interference and access.

We will, as soon as practicable and in accordance with the law, destroy or de-identify any Personal Information that is not longer required for our functions.

Notifiable data breaches

Amendments to The Privacy Act 1988 (Cth) February 22 2018 requires mandatory notification of eligible data breaches.

Occurs when;

- Unauthorised access to, or unauthorised disclosure of personal information or a loss of personal information e.g. USB, smart device with access to information
- Likely to resulting serious harm to **one** or more individuals
- Not been able to prevent the likely serious risk with remedial actions

What is serious harm?

Can be psychological, emotional, physical, reputational or other forms of harm

Requires an objective assessment from perspective of a reasonable person in the entity's position

- ✓ Sensitivity of information e.g. financial, medical ,names and addresses
- ✓ Number of security measures protecting the information e.g. device password protected
- ✓ Person or kind of persons who have obtained the information
- ✓ Whether those person could circumnavigate security technology
- ✓ Nature of the harm e.g. access to financial accounts, breach of IT systems
- ✓ Other relevant matters

Serious harm checklist

1. Types of information accessed or lost
2. Circumstances of the breach
3. Nature of harm that could result

Exceptions to report - remedial actions

If there has been a breach and action is taken before access to or disclosure of information causes serious harm

As a result reasonable person not likely to think there would be serious harm

Suspected data breach

Suspect a data breach that may result in serious harm

Max 30 days to conduct assessment

Must be reasonable and expeditious

Completion of the electronic notifiable data breach form on the office of the Australian Information Commissioner (OAIC) website.

Actions

Maintain Security of personal information

Possible Data Breach

Take immediate steps to contain the data breach

- First priority, take immediate steps to contain the possible data breach.

Conduct an assessment – is the breach likely to result in serious harm of any individuals whose information is involved-

- If you have reasonable grounds to believe there is an eligible breach you must notify if you have reasonable grounds to suspect an eligible breach, you must conduct a reasonable and expeditious assessment of whether there is a notifiable breach, usually within 30 days.

Take remedial action –take possible steps to reduce likelihood of harm to affected individuals caused by the breach

- This might involve recovering the information ,or providing assistance to affected individuals
- If remedial action is able to make serious harm not likely, then notification is not required, and entities can proceed directly to review

Notify – notify individuals likely to suffer serious harm and Australian Information Commissioner

The notification must contain the entity's contact details, a description of the breech, the kind of information concerned, and recommended steps for the individuals.

- if practical notify individuals directly, if not practical you can publish a statement on your website, and take steps to draw attention of the relevant individuals.

Review –Processes and protections

- Consider how the breach occurred and whether to enhance your personal information security measures.

Media

No employee shall make any statement to the press, radio or television stations or to any reporter for the media. If an employee is approached to make a statement or comment they must refer the person to our Chief Executive Officer.

Grievance procedure

If you wish to make a complaint about the way we have managed your Personal Information you may make that complaint verbally or in writing by setting out the details of your complaint to any of the following:

✓ *Our Privacy Officer:* (interim contact is CFO)
Compliance Officer TBA
Phone: 3340 3200
Email: TBA

Or

✓ **Chief Financial Officer (CFO)**
Phone: 07 3340 3200
Email: irmah@sccqld.com.au

Alternatively, complaints may also be referred to a number of services as set out below:

✓ *The Australian Information Commissioner:*
Enquiries by phone: on 1300 363 992

The Australian Information Commissioner receives complaints under the Privacy Act. Complaints can be made in writing:

Online: http://www.oaic.gov.au/privacy/making-a-privacy-complaint
By fax: on +61 2 9284 9666
Email: enquiries@oaic.gov.au

Postal address:
Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

OR

Office of the Australian Information Commissioner
GPO Box 2999
Canberra ACT 2601 NSW 2001

✓ *Aged Care Complaints commissioner*

The Aged Care Complaints commissioner is a independent statutory office holder responsive for providing fee complaints resolution service across Australia. The Complaints Commissioners primary functions under the Aged Care Act 1997 and Complaints Principles 2015.

Online: www.agedcarecomplaints.gov.au

By phone: on 1800 550 552.

If you need an interpreter you can phone the Translating and Interpretation Service on 131 450 and ask to be put through to the Aged Care Complaints Scheme on 1800 500 552.

Hearing or speech impaired TTY users phone 1800 555 677 then ask for 1800 550 552.

For Speak and Listen users phone 1800 555 727 then ask for 1800 550 552.

For internet relay users connect to https://www.iprelay.com.au/call/index.aspx and enter 1800 550 552.

In writing:
Aged Care Complaints Commissioner
GPO Box 9848
(your Capital State or Territory)

How we will deal with your complaint

The complaint will be investigated by us in accordance with our internal procedures and processes.

The complainant may be invited to participate in a conference by the employee conducting the investigation. At the discretion of the service manager other interested parties may also be invited to participate in the conference to discuss the nature of the complaint and attempt to resolve it. This may include the presence or participation of a support person or advocate for the complainant.

The complainant will be provided with a response to their complaint within a reasonable timeframe after completion of any investigation. The response will be in writing and will include the outcome of the investigation, any proposed action and details of the right to lodge a complaint with any relevant external Organisations.

Privacy Officer

We have appointed a Privacy Officer to manage and administer all matters relating to protecting the privacy of individuals' Personal Information.

The Privacy Officer can be contacted if any relevant person wishes to obtain more information about any aspect of this policy or about the way in which we operate to protect the privacy of individuals' Personal Information.

As stated above, complaints may also be made to the Privacy Officer if any person suspects we have breached this privacy policy, the Australian Privacy Principles or they are otherwise unhappy with the management of their (or if they are responsible for another person, that person's) Personal Information.