

# PRIVACY POLICY



---

## PRIVACY POLICY

### 1 POLICY

We will use all reasonable efforts to protect the privacy of individuals' personal information and to comply with the obligations imposed by the *Privacy Act 1988* (Cth) (**Privacy Act**) including the Notifiable Data Breach (NDB) amendments, the Australian Privacy Principles (**APPs**), the Aged Care Act and the Aged Care Principles.

This policy applies to all Residents and Staff (including contracted agency staff) and Volunteers.

We will only collect personal information by lawful and fair means and will only collect personal information that is necessary for one or more of our organisation's functions or activities.

If it is reasonable and practicable to do so, we will collect personal information about an individual only from that individual, or authorised government agencies.

In meeting our obligations with respect to the privacy of our clients we acknowledge that people with vision or hearing impairments and those of culturally and linguistically diverse people may require special consideration.

### 2 PURPOSE OF POLICY

The purpose of this policy and procedure is to:

- i) ensure personal information is managed in an open and transparent way;
- ii) protect the privacy of personal information including Health Information of clients, residents and staff;
- iii) provide for the fair collection and handling of personal information;
- iv) ensure that personal information we collect is used and disclosed for relevant purposes only;
- v) regulate the access to and correction of personal information; and
- vi) ensure the confidentiality of personal information through appropriate access, storage and security.

### 3 Definitions

#### **What is “Personal Information”?**

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.

#### **What is “Sensitive Information”?**

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.

#### **What is “Health Information”?**

Health Information is:

- i) information or an opinion about:
  - A. the health or a disability (at any time) of an individual;
  - B. an individual’s expressed wishes about the future provision of health services to him or her; or
  - C. a health service provided, or to be provided, to an individual that is also personal information; or
- ii) other personal information collected to provide, or in providing, a health service;
- iii) 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; or
- iv) 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.

#### **What is “Unsolicited Information”?**

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

#### **What is an “Employee Record”?**

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 personal information about all or any of the following:

- i) the engagement, training, disciplining or resignation of the employee;

- ii) the termination of the employment of the employee;
- iii) the terms and conditions of employment of the employee;
- iv) the employee's personal and emergency contact details;
- v) the employee's performance or conduct;
- vi) the employee's hours of employment;
- vii) the employee's salary or wages;
- viii) the employee's membership of a professional or trade association;
- ix) the employee's trade union membership;
- x) the employee's recreation, long service, sick, personal, maternity, paternity or other leave;
- xi) the employee's taxation, banking or superannuation affairs;
- xii) photo id and biometric data.

### **What is a "Resident Record"?**

A Resident Record is a record of personal information relating to the care of the resident. Examples of resident information relating to the care of the resident are Health Information about the resident and personal information about all or any of the following:

- i) the resident's financial records;
- ii) the resident's health records;
- iii) power of attorney documents
- iv) guardianship order/s
- v) banking details
- vi) next of kin

## **4 COLLECTION, USE AND DISCLOSURE**

We will collect and use information about you during the course of your relationship with us. We explain below when and 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.

## **5 COLLECTION OF PERSONAL INFORMATION**

### **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 and collection of the Personal Information is necessary to:

- i) comply with the provisions of state or commonwealth law;
- ii) provide data to government agencies in compliance with state or commonwealth law;

- iii) determine eligibility to entitlements provided under any state or commonwealth law;
- v) provide appropriate services and care;
- vi) enable contact with a nominated person regarding a client's health status;
- vii) 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:

- i) you have consented to the collection of this information; or
- ii) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or
- iii) a permitted general situation exists to the collection of the information; or a permitted health situation exists in relation to the collection of the information;

## 6 METHODS OF COLLECTION

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

- i) from a client, resident or employee;
- ii) from any person or organisation that assesses health status or care requirements, for example the Aged Care Assessment Team;
- iii) from the health practitioner of a client or resident;
- iv) from other health providers or facilities;
- v) from family members or significant persons of a client or resident; and
- vi) from a legal advisor of a client or resident;
- vii) from the ATO or relevant government departments;
- viii) our website, social media and other online platforms;
- ix) Telephone/fax communications
- x) Video footage via CCTV recordings whilst on premises

We will collect Personal Information from the client or resident unless:

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

At admission, staff, client or resident's should identify any parties from whom they do not wish Personal Information accessed or to whom they do not wish Personal Information provided. This

should be recorded in the file of the client or resident 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.

### **Electronic communications**

Where possible, encryption is enabled between server and endpoints. Transmission of information via the internet has inherent risks. You should be aware of the risks when sending personal information, to any party, via email or via web. If you are concerned of the risks then you may use other methods of communication, such as post, fax or phone.

### **Personal records**

We must keep a record in respect of staff about:

- i) basic employment details such as the name of the employer and the employee and the nature of their employment (eg part-time, full-time, permanent, temporary or casual);
- ii) pay;
- iii) overtime hours;
- iv) averaging arrangements;
- v) leave entitlements;
- vi) superannuation contributions;
- vii) termination of employment (where applicable);
- viii) individual flexibility arrangements and guarantees of annual earnings; and
- ix) photographs video/audio recordings and biometric data.

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

### **Resident records**

We must keep a record in respect of residents about:

- i) financial details;
- ii) next of kin details;
- iii) Centrelink details;
- iv) Department of veteran affairs;
- v) Power of attorney/guardianship details;

- vi) Medical details; and
- vii) Will;

## **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:

- i) our identity and contact details;
- ii) the purpose for which we are collecting Personal Information;
- iii) the identity of other entities or persons to whom we usually disclose Personal Information to;
- iv) that our privacy policy contains information about how the individual may complain about a breach of the APPs and how we will deal with a complaint;
- v) 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**

### **a) Permitted disclosure**

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

- i) 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;
- ii) 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;
- iii) 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;
- iv) 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;
- v) 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
- vi) 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.

#### **b) 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:

- i) 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;
- ii) we reasonably believe the disclosure is necessary or authorised by Australian Law; or
- iii) the individual has provided express consent to the disclosure.

#### **c) Disclosure of Health Information**

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

- i) the individual is incapable of giving consent or communicating consent;
- ii) 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
- iii) the disclosure is not contrary to any wish previously expressed by the individual of which 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.

## **7 ACCESS**

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

- i) is frivolous or vexatious;
- ii) poses a serious threat to the life or health of any individual;
- iii) unreasonably impacts upon the privacy of other individuals;
- iv) jeopardises existing or anticipated legal proceedings;

- v) prejudices negotiations between the individual and us;
- vi) be unlawful or would be likely to prejudice an investigation of possible unlawful activity;
- vii) an enforcement body performing a lawful security function asks us not to provide access to the information; or
- viii) 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:

- i) there is a serious threat to life, health, or harm of any individual;
- ii) the privacy of others may be affected;
- iii) the request is frivolous or vexatious;
- iv) the information relates to existing or anticipated legal proceedings; or
- v) 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**

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

## **8 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, or wish to change any aspect of the information we hold.



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

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

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.

## 10 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:

- i) you would reasonably expect us to use or disclose your Personal Information for the purpose of direct marketing; and
- ii) 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 an 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:

- i) ask us not to provide direct marketing communications to them;
- ii) ask us not to disclose or use the information;
- iii) ask us to provide the source of the information.

## 11 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, from unauthorised access, modification or disclosure.

## **Information of a Client or Resident**

- i) We must keep the records of a client or resident in a secure storage area, where records are stored electronically access controls are in place to prevent unauthorised access.
- ii) If the records are being carried while providing care only the staff member carrying the records will have access to them.
- iii) Records of previous clients and residents and earlier unused volumes of current clients or residents shall be archived and stored in a locked service away from general use.
- iv) Only health professionals attending to the care of a client or resident are to have access to information of the client or resident. All records shall only be used for the purpose it was intended.
- v) A client or resident, or their representatives shall be provided access to records as requested and after consultation with the service manager. At these times, a qualified staff member is to remain with a client or resident or representative to facilitate the answering of any questions raised.
- vi) Details of a client or resident are not to be provided over the phone, unless the staff member is sure of the person making the inquiry. If in doubt, consult the service manager.
- vii) No staff shall make any statement about the condition or treatment of a client or resident to any person not involved in the care except to the immediate family or representative of the client or resident and then only after consultation with the service manager.
- viii) All staff must be discreet with their comments at all times, protecting and respecting the privacy, dignity and confidentiality of all clients and residents.
- ix) Handovers shall be conducted in a private and confidential manner.

## **Security measures**

Our security measures include, but are not limited to:

- (i) training our staff on their obligations with respect to Personal Information;
- (ii) use of passwords when accessing our data storage system; and
- (iii) the use of firewalls, intrusion detection and virus scanning tools to protect against unauthorised interference and access.

This applies to staff (including contracted staff) who are required to have up-to-date virus protection software and firewalls installed on any device used to access documents containing Personal Information.

Contractors working on our behalf are required to:

- (i) comply with the Australian Privacy Principles;
- (ii) have up-to-date virus protection software and firewalls installed on any device used to access documents containing Personal Information;
- (iii) notify us of any actual or potential breaches of security;

- (iv) indemnify us in relation to any loss suffered by a breach.

We will, as soon as practicable and in accordance with the law, destroy or de-identify any Personal Information that is no longer required for our functions.

## 12 MEDIA

No member of staff shall make any statement to the press, radio or television station or to any reporter for the media. If a staff member is approached to make a statement or comment, they must refer the person to the CEO.

## 13 GRIEVANCE PROCEDURE

### How to make a complaint

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:

**(a) The CEO**

Phone: (02) 9764 7800

Email: [columbia@cnh.com.au](mailto:columbia@cnh.com.au)

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

**(b) Office of the Australian Information Commissioner**

Office of the Australian Information Commissioner receives complaints under the Act. Complaints can be made:

Online: <http://www.oaic.gov.au/privacy/making-a-privacy-complaint>

By phone: on 1300 363 992

By fax: on +61 2 9284 9666

By email: [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au)

In writing:

Address your letter to the Australian Information Commissioner at the:

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

### **(c) Aged Care Complaints Commissioner**

The Aged Care Complaints Commissioner operates within the Department of Social Services receives complaints under the Act. Complaints can be made:

Online: <https://www.agedcarecomplaints.gov.au/internet/accc/publishing.nsf/Content/Home>

By phone: on 1800 550 552.

Or if you need an interpreter you can phone the Translating and Interpretation Service on 131 450 and ask them to put you through to the Aged Care Complaints Commissioner on 1800 550 552.

For 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://internet-relay.nrscall.gov.au/> and enter 1800 550 552.

In writing:

Address your letter to the Aged Care Complaints Commissioner at

the: Aged Care Complaints Commissioner  
GPO Box 9848  
SYDNEY NSW 2000

### **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 staff member conducting the investigation. At the discretion of the Facility 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. This 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.

## **14 PRIVACY OFFICER**

We have appointed a Privacy Officer to manage and administer all matters relating to protecting the privacy of individual's 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 individual's 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.

### **Accidental or unauthorised disclosure of personal information**

We will take seriously and deal promptly with any accidental or unauthorised disclosure of personal information. We will follow the OAIS's Data Breach Notification, when handling accidental or unauthorised information disclosure.

### **Privacy Policy updates**

This privacy policy will be reviewed frequently and updated as required.

### **Other Associated Documents**

**PFC 38** Data Breach

Suspected Data Breach Checklist