1.5 Client Privacy & Confidentiality Policy & Procedure

1. Policy

Value Care is committed to ensuring that all clients and external stakeholders of the organisation have the same level of privacy, dignity and confidentiality as is expected by the rest of the community.

The purpose of this policy is to establish standards of privacy, dignity and confidentiality in the organisation's dealings with prospective, current and past users of the organisation's services. The policy has been framed around individuals' rights as they are specified in the Privacy Act (1988), Freedom of Information Act (1982), Disability Services Act (1993) and the Home Care Standards.

- All information relating to clients and Value Care is confidential and shall not be used or disclosed to sources other than those authorised by the Managing Director. Where there is a need to release individual client or nursing agency information, written consent will be obtained by the Managing Director and staff notified appropriately.

- The actions of each staff member, in relation to privacy of information, are governed by the relevant sections of the *Privacy Act* 1988 (Commonwealth) which includes the Privacy Amendment (Private Sector) Act 2000 (Commonwealth). These provisions and principles apply in addition to any other obligation found within State laws.

- Only authorised staff members are to have access to information relevant to either an individual client or the organisation.

- All confidential information within the office environment is to be kept in a locked and secure manner.

- Client care records are maintained within the client's home environment and must be stored in a safe, out of general sight and secure position that is mutually agreed to, by the care recipient and the service provider.

- Whilst ever the record file remains in the client's home it remains the property and legal record of the service provider. A copy of the file may be requested by the care recipient at any time, with mutual consent, however the original legal record/files must be returned to Value Care on discharge. This record is then stored in secure, fireproof storage within the office for a period of seven years.

- Prior to any disclosure of the contents of a client's record, with any other parties, there must be agreement by both the health recipient and the organisation.

- Staff are responsible for ensuring that any written or verbal record is accurate, relevant, up-to-date and complete.

1.1 To whom does this Policy apply?

This policy applies to staff regardless of their position within the organisation

1.2 Distribution of the Policy

This policy forms part of the recruitment process. Updates / changes to the policy will be communicated to staff via the staff newsletter. The policy is located in the Organisational Directions and Standards Manual.

1.3 Expected Outcome/s

- Clients and families are informed why the information sought is required by the organisation.

- Authority to Release Information forms have been completed by clients or families prior to information being collected from other sources.

- Value Care maintains a client information system that houses all personal information pertaining to an individual client in the one locality.

- Client files are stored in a lockable medical records room in a non-public place in the office and files are returned to their proper location as soon as they are no longer required.

- All employees have been provided with access to a copy of the organisation's Policy on Confidentiality and Privacy Policy.

2. Procedure

The staff member responsible for collecting information is required to ensure that the client is aware of the purpose for which the information is collected.

Staff are to ensure that the information collection process does not intrude to an unreasonable extent on the personal affairs of the individual. Only information pertaining to nursing and / or homecare of the client is relevant and permitted to be obtained.

Staff are required to complete a Deed of Confidentiality on commencement of employment with Value Care.

Value Care provides a wide range of services and collects personal information to ensure a holistic approach to the care and services we offer. We recognise and respect every person's right to privacy, dignity and confidentiality.

Value Care will therefore:

- Provide environments that enable residents & clients to maintain relationships with privacy and dignity.
- Develop practices to enable residents & clients to undertake personal activities with privacy.
- Promote respectful relationships between all staff, residents, clients and their representatives.
- Ensure compliance with the Privacy Act 1988 (The Act) and the 13 Australian Privacy Principles (APPs) outlined in the Act in all facets of our operations.

3. Principles

3.1 Transparency

We will be open about how we manage personal information. If asked, we will provide information on our approach to privacy.

3.2 Personal Information

Personal information is defined by the Act as information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not. Examples of personal information might include an individuals' name, address, phone number, email address, medical records, family details or any other information from which an individual could reasonably be identified.

Clients have the right to not identify themselves or use a pseudonym when requesting services. However, this will not apply if it is impracticable for Value Care to provide services to the individual.

We may collect a variety of personal information relating to the provision of our services. Examples of personal information which we regularly collect include an individual's:

* name;

* address;

* contact details;

* date of birth;

* marital status;

* family details, including personal information about an individual's next of kin;

* health and medical details

* Medicare number

* financial details; or

Other personal information particular to a specific individual to allow us to tailor our services to that individual.

3.3 Collection

We will collect the personal information we need to provide and market our services. We will use fair and lawful ways to collect it.

We will usually ensure we have consent to collect sensitive information.

Where reasonably practicable, we will attempt to collect personal information directly from individuals, however, in some cases this may be impracticable, or the information may be held by a third party.

Common examples of these situations may include:

- medical records held by an individual's current or previous health care provider;
- financial records held by an accountant or Centrelink; or
- next of kin details.

When collecting information, we will take reasonable steps to let individuals know why we are collecting it, who we will give it to and how we will use or disclose it.

While an individual chooses not to provide personal information to us, it may hamper the provision of services. In some case failure to provide personal information may result in us being incapable of providing services to an individual.

3.4 Use and Disclosure

We will usually only use or disclose personal information:

- for the primary purpose for which it was collected;
- for related purpose which the individual would reasonably expect; or
- with consent.

Some examples of situations where we may use an individual's personal information include:

- assessing potential eligibility for our services;
- determining deposits or other amounts payable by an individual for the provision of our services;
- corresponding with an individual regarding the services being provided, including regarding an individual's satisfaction with the services;
- tailoring our services to an individual's specific needs;
- discussing the services being provided to an individual with the individual's family or next of kin; or

We may also use or disclose non sensitive personal information for a secondary purpose (such as research or marketing) if:

- the individual has consented, or
- where it is impracticable to seek consent before this use (assuming consent has not already been denied). In such cases, the individual is given the opportunity to opt out of further communications.

Situations where Value Care may use or disclose information without an individual's consent include:

- where we reasonably believe that use or disclosure is necessary to reduce or prevent a threat to a person's life, health or safety or a serious threat to public health or safety;
- where we are investigating or reporting on suspected unlawful activity;
- where the use or disclosure is required by law;
- where we reasonably believe that the use is necessary for law enforcement, public revenue protection, prevention and remedying of serious improper conduct, or conduct of court or tribunal proceedings, either by or on behalf of an enforcement body.

We will not provide an individual's personal information to any overseas entity unless required by law.

If we use or disclose information without consent, we will record each instance in writing.

3.5 Data Quality

We will take reasonable steps to ensure that the personal information we hold is accurate and current. We will contact clients where necessary to confirm their personal information.

3.6 Data Security

We will implement measures to protect personal information from misuse, loss, unauthorised access, changes or disclosure.

We will destroy or permanently de-identify personal information when we no longer need it.

We will protect the security of information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information that clients input.

3.7 Accessing and Correcting Personal Information

Usually, when asked, we will give an individual access to their personal information. However, we may deny a request for access if we reasonably believe:

- It would pose a serious or imminent threat to the life or health of any person.
- The privacy of others would be unreasonably affected.
- The request is frivolous or vexatious.
- The information relates to existing legal proceedings with the person who is the subject of the information and would not be accessible through discovery.
- Providing access would prejudice negotiations with the person who is the subject of the information by revealing our intentions regarding those negotiations.
- Providing access would be unlawful or denying access is required or authorised by law.
- Providing access would be likely to prejudice an investigation of unlawful activity or law enforcement, public revenue protection, prevention and remedying of seriously improper conduct, or preparation or conduct of court or tribunal proceedings, either by or on behalf of an enforcement body.
- An enforcement body performing a lawful security function requests denial of access to protect national security.
- Where evaluative information generated by us in making a commercially sensitive decision would be revealed by providing access.

If we refuse access, we will explain why.

An individual may request access to their personal information by contacting us using the details contained at the end of this document.

When requesting access or correction of personal information we will require an individual to verify their identity by reference to their personal information. In some circumstances it may be necessary for an individual to visit one of our locations to properly verify their identity.

Generally, we will not charge a fee to grant access to information, however in the case of requests for old or particularly voluminous information it may be necessary for us to charge a reasonable fee, commensurate with the work required to comply with the request. However, there will be no fee charged in relation to the making of the request for access itself.

In addition to requesting access to personal information an individual may request that we correct any personal information held about them.

3.8 Identifiers

We will not adopt Commonwealth Government identifiers for use as our own identifiers. If we are required to collect a government identifier in providing our services to individuals, we will not use this number to identify the individual.

3.9 Anonymity or Pseudonymity

If reasonably possible, we will give individuals the option of dealing with us anonymously or by use of a pseudonym. However, we cannot provide services to someone without confirming their identity. We will be able to discuss our services in a general way, including costs and charges which we might ordinarily charge for those services, prior to obtaining an individual's identity. Until such time as we has been provided sufficient information to provide a detailed quotation or outline of services to an individual any communication will be general in nature and will not be binding upon us.

3.10 Sensitive Information

Generally, we will only collect sensitive information with an individual's consent, except where:

* The collection is required or authorised by law or to establish, exercise or defend a legal or equitable claim, or;

* It is necessary to prevent or lessen a serious or imminent threat to the life or health of the person who is the subject of the information.

3.11 Donations

ValueCare gathers and retains personal information from donors and that information is managed in compliance with the Payment Card Industry Security Data Standard.

Our donations system and the information it contains are held internally and we do not release that information for external use at all. Donation processing is secured by 128-bit SSL encryption to protect the transfer of personal and financial information. Each donation is secured, and credit card details are not stored at any time. The only information collected and retained is the amount donated, transaction date and contact details as completed on the donation form

Where donations are made over the phone or via email, a copy of that donation is retained for tax and audit purposes in a secure location.

3.12 Complaints

If an individual wishes to make a complaint about our collection, use or disclosure of any personal information, or about any potential breach of an APP, they may contact the Privacy Compliance Officer by use of the contact details at the end of this document.

When making a complaint an individual should include as many details as possible, including the nature of the personal information, how it is believed to have been misused, which APP is believed to have been breached (if relevant), the details of any of our employees or representatives involved and any other information which may be relevant. The Privacy Compliance Officer may request additional information to enable them to properly investigate the complaint and take reparatory action.

Once a complaint is received the Privacy Compliance Officer will investigate and determine whether a misuse of personal information has occurred, how it may be rectified and what action should be taken in relation to any of our employees or representatives involved. We will endeavour to keep the individual informed regarding the process of their complaint and any action taken.

Should an individual not be satisfied with our handling of their complaint we will generally agree to the complaint being referred to mediation and/or arbitration. Should the matter remain unresolved then an individual is entitled to refer their matter to the Office of the Australian Information Commissioner.

3.13 Internet Privacy

Visitors to our website are informed of our Internet Privacy Policy, replicated below.

“By using this site, you agree to the Internet Privacy Policy of this web site ("the web site"), which is set out on this web site page. The Internet Privacy Policy relates to the collection and use of personal information you may supply to us through your conduct on the web site and should be read in conjunction with our general Privacy Policy, above.

We reserve the right, at our discretion, to modify or remove portions of this Internet Privacy Policy at any time. This Internet Privacy Policy is in addition to any other terms and conditions applicable to the web site. We do not make any representations about third party web sites that may be linked to the web site.

We recognise the importance of protecting the privacy of information collected about visitors to our web site, in particular information that is capable of identifying an individual ("personal information"). This Internet Privacy Policy governs the manner in which your personal information, obtained through the web site, will be dealt with. This Internet Privacy Policy should be reviewed periodically so that you are updated on any changes. We welcome your comments and feedback”.

3.14 Personal Information

Personal information about visitors to our site is collected only when knowingly and voluntarily submitted. For example, we may need to collect such information to provide you with further services or to answer or forward any requests or enquiries. It is our intention that this policy will protect your personal information from being dealt with in any way that is inconsistent with applicable privacy laws in Australia.

3.15 Use of Information

Personal information that visitors submit to our site is used only for the purpose for which it is submitted or for such other secondary purposes that are related to the primary purpose, unless we disclose other uses in this Internet Privacy Policy or at the time of collection. Copies of correspondence sent from the web site, that may contain personal information, are stored as archives for record-keeping and back-up purposes only.

3.16 Collecting information on registered members

As part of registering with us, we collect personal information about you in order for you to take full advantage of our services. To do this it may be necessary for you to provide additional information to us as detailed below.

3.17 Registration

Registration is completely optional. Registration may include submitting your name, email address, address, telephone numbers, option on receiving updates and promotional material and other information. You may access this information at any time by contacting our office.

3.18 Credit Card Detail

This ensures that payment card information is kept confidential and secure, and that there is compliance with the Payment Card Industry Data Security Standard.

3.19 Disclosure

Apart from where you have consented or disclosure is necessary to achieve the purpose for which it was submitted, personal information may be disclosed in special situations where we

have reason to believe that doing so is necessary to identify, contact or bring legal action against anyone damaging, injuring, or interfering (intentionally or unintentionally) with our rights or property, users, or anyone else who could be harmed by such activities. Also, we may disclose personal information when we believe in good faith that the law requires disclosure.

We may engage third parties to provide you with goods or services on our behalf. In that circumstance, we may disclose your personal information to those third parties in order to meet your request for goods or services.

3.20 Security

We strive to ensure the security, integrity and privacy of personal information submitted to our sites, and we review and update our security measures in light of current technologies. Unfortunately, no data transmission over the Internet can be guaranteed to be totally secure.

However, we will endeavour to take all reasonable steps to protect the personal information you may transmit to us or from our online products and services. Once we do receive your transmission, we will also make our best efforts to ensure its security on our systems.

In addition, our employees and the contractors who provide services related to our information systems are obliged to respect the confidentiality of any personal information held by us. However, we will not be held responsible for events arising from unauthorised access to your personal information.

3.21 Notifiable Data Breaches

The Privacy Amendment (Notifiable Data Breaches) Act 2017 requires us to notify the relevant parties if there is an eligible data breach. This means we will let you know in the way we normally communicate with you, if:

- There is unauthorised access to or disclosure of your information; or your information is lost, and unauthorised access or disclosure is likely to occur; and
- There is a reasonable chance that this could cause you serious harm (which can include physical, physiological, emotional, economic or reputational harm); and
- We have been unable to remedy the situation in line with the Act.

If we are unable to contact any affected parties individually, we will post a notification that an eligible data breach has occurred on our website.

In such circumstances we are also required to inform the Office of the Australian Information Commissioner.

We will follow our Notifiable Data Breach Procedure in these instances.

4. Collecting Information from Users

4.1 IP Addresses

Our web servers gather your IP address to assist with the diagnosis of problems or support issues with our services. Again, information is gathered in aggregate only and cannot be traced to an individual user.

We will never (and will not allow any third party to) use the statistical analytics tool to track or to collect any Personally Identifiable Information (PII) of visitors to our site. Google will not associate your IP address with any other data held by Google. Neither we nor Google will link, or seek to link, an IP address with the identity of a computer user.

We will not associate any data gathered from this site with any Personally Identifiable Information from any source, unless you explicitly submit that information via a fill-in form.

4.2 Access to Information

We will endeavour to take all reasonable steps to keep secure any information which we hold about you, and to keep this information accurate and up to date. If, at any time, you discover that information held about you is incorrect, you may contact us to have the information corrected.

In addition, our employees and the contractors who provide services related to our information systems are obliged to respect the confidentiality of any personal information held by us.

4.3 Links to other sites

We provide links to Web sites outside of our web sites, as well as to third party Web sites. These linked sites are not under our control, and we cannot accept responsibility for the conduct of companies linked to our website. Before disclosing your personal information on any other website, we advise you to examine the terms and conditions of using that Web site and its privacy statement.

4.4 Problems or questions

If we become aware of any ongoing concerns or problems with our web sites, we will take these issues seriously and work to address these concerns. If you have any further queries relating to our Privacy Policy, or you have a problem or complaint, please contact us.

For more information about privacy issues in Australia and protecting your privacy, visit the Office of the Australian Information Commissioner's web site; http://www.oaic.gov.au/.

5. Further Information

Persons requiring further information about privacy at Value Care should contact our office on Phone: 02 9635 4744 or email us on Email: contact@valuecare.org.au

5.1 Definitions and Abbreviations

APP = Australian Privacy Policy

Document Information and Revision History {DIRH}

Document Title	1.5 Privacy & Confidentiality Policy & Procedure
Original Author(s)	I.Thakkar, S. Kumar
Current Revision Author(s)	I.Thakkar

Revision History

Revision	Date	Author(s)	Notes
1	July 2020	I.Thakkar	Insertion of DIRH
2			
3			
4			
5			
6			
7			
8			