ORG-REC-001 Privacy and Confidentiality

POLICY			
Approved by:	CEO	**Approval Date:**	3/03/2017
Date Effective:	03/03/2017	**Next Review Due:**	3/03/2020
Custodian:	CEO		
Employer:	The CareSouth Group is comprised of the below entities, collectively known as the CareSouth Group. Other entities may be added in the future to the CareSouth Group. This policy applies to staff, volunteers and contractors employed in each of these entities. • CareSouth ABN 97 065 193 035 • CareSouth Residential OOHC ABN 19 164 554 607 • CareSouth Foster Care ABN 32 164 554 223 • CareSouth Family Connections ABN 93 164 553 799 • CareSouth Disabilities ABN 32 164 553 413		
System Location:	S:\Common\CareSouth_Policies\2. Organisational		
Related Material:	**CARESOUTH POLICIES AND DOCUMENTS** This policy has been written with reference to and operates in conjunction with the following CareSouth policies and procedures: • *Complaints and Feedback Policy and Procedure* • *DIS-014 Client Decision-Making and Consent Policy* • *ORG-IT-001 Information Technology Security Policy* • *ORG-REC-002 Records Management Policy* • *ORG-REC-003 Subpoena Compliance Policy* • *ORG-REC-004 Workplace Surveillance Policy* • *ORG-REC-006 Exchange of Information policy* • *ORG-REC-008 Client Access to Records Policy* • *PRO-DIS-006 Client Decision-Making and Consent Procedure* • *PRO-ORG-REC-002 Records Management Procedure* • *PRO-ORG-REC-003 Subpoena Compliance Procedure* • *PRO-ORG-REC-006 Exchange of Information Procedure*		

	• *PRO-ORG-REC-008 Client Access to Records Procedure* **LEGISLATION AND EXTERNAL STANDARDS** This policy has been written with reference to and operates in conjunction with the following legislation and external standards: • *Privacy Act 1988 (Cth)* • *Privacy Amendment (Private Sector) Act 2000 (Cth)* • *Privacy Amendment (Enhancing Privacy Protection) Act 2012* • *Spam Act 2003 (Cth)* • *Privacy and Personal Information Protection Act 1998 (NSW)* • *Health Records and Information Privacy Act 2002 (NSW)* • *Health Records (Privacy and Access) Act 1997 (ACT)* • *Freedom of Information Act 1989 (ACT)* • *Territory Records Act 2002 (ACT)*

TABLE OF CONTENTS

1. PURPOSE 3
2. SCOPE & APPLICATION 3
3. DEFINITIONS 4
4. POLICY 10
4.1. Collection of personal information 11
4.2. Consents to information collection and use 12
4.3. Use and disclosure of personal information 12
4.4. Exchange of personal information with third parties 14
4.5. Marketing 16
4.6. Cross-border disclosure of personal information 16
4.7. Access restrictions and security of personal information 17
4.8. Quality of personal information 19
4.9. Client and family member access to personal information 19
4.10. Correction of personal information 19
4.11. Privacy complaints 19
5. RESPONSIBILITIES 20
5.1. Employees, Volunteers, Students, Contractors, Consultants 20
5.2. Managers 20
6. AUTHORITY 20
7. VERSION CONTROL AND CHANGE HISTORY 21

1. PURPOSE

This policy outlines CaresSouth's practices governing the collection and handling of personal data about our clients, carers and employees, including how it collects, uses, stores, discloses and protects information about individuals and families.

This policy outlines how CareSouth meets its legislative requirements and the Australian Privacy Principles as follows:

- APP 1 — Open and transparent management of personal information
- APP 2 — Anonymity and pseudonymity
- APP 3 — Collection of solicited personal information
- APP 4 — Dealing with unsolicited personal information
- APP 5 — Notification of the collection of personal information
- APP 6 — Use or disclosure of personal information
- APP 7 — Direct marketing
- APP 8 — Cross-border disclosure of personal information
- APP 9 — Adoption, use or disclosure of government related identifiers
- APP 10 — Quality of personal information
- APP 11 — Security of personal information
- APP 12 — Access to personal information
- APP 13 — Correction of personal information

In addition to the above requirements, CareSouth has a responsibility to protect its clients under the Children and Young Persons (Care and Protection) Act 1998 and other relevant child welfare frameworks such as those managed by the NSW Ombudsman, Children's Guardian and Commissioner for Children. This requires that in specific circumstances, CareSouth has a legal responsibility to request, disclose and use personal information about carers, applicants for employment, children and young people.

2. SCOPE & APPLICATION

This policy applies to all employees and volunteers during the course of their work for CareSouth, conducted in CareSouth workplaces within NSW or the ACT. It applies to all personal information about its clients, carers, volunteers and employees that CareSouth handles.

3. DEFINITIONS

Term	Definition
Capacity	An individual must have the *capacity* to consent. This means that the individual is capable of understanding the nature of a consent decision, including the effect of giving or withholding consent, forming a view based on reasoned judgement and how to communicate a consent decision. Issues that could affect an individual's capacity to consent include age, physical or mental disability, temporary incapacity (for example, during a psychotic episode, a temporary psychiatric illness, or because the individual is unconscious, in severe distress or suffering dementia), and limited understanding of English.
Client	Children, young people, families and people with disability using our services.
Collection	The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means, including from individuals, other entities, generally available publications, surveillance cameras, information associated with web browsing, such as personal information collected by cookies, and biometric technology, such as voice or facial recognition. Collection may also take place when an organisation generates personal information from other data it holds, such as the generation of an audit log.
Consent	The main criteria for establishing consent are: • the individual is adequately informed before giving consent • the individual gives consent voluntarily • the consent is current and specific, and • the individual has the capacity to understand and communicate their consent.

Term	Definition
Court/tribunal order	'Court/tribunal order' is defined as an order, direction or other instrument made by a Commonwealth, State or Territory court, a tribunal, a judge, a magistrate, a person acting as a judge or magistrate, a member or an officer of a tribunal, and a judge or magistrate who has been appointed by government to an office or inquiry that involves the exercise of administrative or executive functions, including functions that are quasi-judicial in nature (an example is a judge who is appointed by government to conduct a royal commission).
Data breach	A data breach is when personal information held by an organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. Examples of a data breach are when a device containing clients' personal information is lost or stolen, an organisation's database containing personal information is hacked or an organisation mistakenly provides personal information to the wrong person.
De-identification	Personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.' De-identification involves removing or altering information that identifies an individual or is reasonably likely to do so. Generally, de-identification includes two steps: • removing personal identifiers, such as an individual's name, address, date of birth or other identifying information, and • removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.
Direct marketing	Direct marketing involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services. A direct marketer may communicate with an individual through a variety of channels, including telephone, SMS, mail, email and online advertising.

Term	Definition
Disclosure	An organisation discloses personal information when it makes it accessible or visible to others outside the organisation, and releases the subsequent handling of the personal information from its effective control. The release may be a proactive release, a release in response to a specific request, an accidental release or an unauthorised release by an employee.
Employees	Includes CareSouth Board Members, paid employees, volunteers, students and contractors.
Government Identifier	An identifier is a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual. A government related identifier is an identifier that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a contracted service provider for a Commonwealth or State contract. An identifier will be personal information if the individual is identifiable or reasonably identifiable from the identifier, including from other information held by, or available to, the organisation that holds the identifier.
Health information	Information or an opinion, that is also personal information, about: • the physical or psychological health or a disability (at any time) of an individual • an individual's expressed wishes about the future provision of health services • a health service provided, or to be provided, to an individual • 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 their 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.

Term	Definition
Health service	An activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it: • to assess, record, maintain or improve the individual's health • to diagnose or treat the individual's actual or suspected illness or disability • the dispensing or prescription of a drug or medicinal preparation by a pharmacist. An above activity that takes place in the course of providing care for a person with a disability is a health service.
Holds	An organisation 'holds' personal information if 'the organisation has possession or control of a record that contains the personal information'. An organisation 'holds' personal information where: • it physically possesses a record containing the personal information and can access that information physically or by use of an electronic device (such as decryption software) • it has the right or power to deal with the personal information, even if it does not physically possess or own the medium on which the personal information is stored. For example, the organisation has outsourced the storage of personal information to a third party but it retains the right to deal with it, including to access and amend that information.

Term	Definition
Personal information	Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable. Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person. Personal information of one individual may also be personal information of another individual. Examples include a marriage certificate that contains personal information of both parties to a marriage, and a vocational reference that includes personal information about both the author and the subject of the reference. Personal information that has been de-identified is no longer considered be personal information.
Record	The term 'record' includes a document or an electronic or other device. Some items are excluded from the definition, such as anything kept in a library, art gallery or museum for the purposes of reference study or exhibition and Commonwealth records in the open access period.

Term	Definition
Sensitive information	'Sensitive information' is a subset of personal information and is defined as 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 political association, professional or trade association or trade union • sexual orientation or practices • criminal record • health information about an individual • genetic information (that is not otherwise health information) • biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or • biometric templates. Sensitive information is generally afforded a higher level of privacy protection under the APPs than other personal information. This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual. For example, discrimination or mistreatment is sometimes based on a person's race or ethnic origin or union membership. Mishandling of sensitive information may also cause humiliation or embarrassment or undermine an individual's dignity.
Unauthorised access	Examples of unauthorised access include a cyber-attack or a theft, including where the third party then makes that personal information available to others outside the entity. An organisation is not taken to have disclosed personal information where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information. However, where a third party gains unauthorised access, the organisation may breach APP 11 if it did not take reasonable steps to protect the personal information from unauthorised access.

Term	Definition
Unsolicited personal information	Personal information received by an organisation where the organisation has taken no active steps to collect the information.
Use	'Use' involves handling and managing the information within the organisation's effective control. Examples include: • accessing and reading the personal information • searching records for the personal information • making a decision based on the personal information • passing the personal information from one part of the organisation to another • unauthorised access by an employee.

4. POLICY

CareSouth is committed to protecting information about individuals, including employees, volunteers, carers and clients.

CareSouth recognises the trust that families, carers, children, young people, and people with disability place in CareSouth, and understands the sensitive nature of the information it collects in the course of providing its services. All employees are trained to understand their legal responsibilities to protect privacy and confidentiality and will be supported through supervision.

The key elements of CareSouth's approach to managing personal information are as follows:

- We collect only information that CareSouth needs in order to provide our services to clients and meet its child protection and welfare obligations.
- We ensure that stakeholders are informed as to why we collect the information and how we administer the information gathered.
- We use and disclose personal information only as required to provide our services and meet our child protection and welfare obligations, or with the individual's consent. This includes collecting information about current and prospective employees, students and volunteers.
- We store personal information securely, protecting it from unauthorised access.
- We provide stakeholders with access to their own information, and the right to seek its correction.

4.1. Collection of personal information

CareSouth only solicits and collects personal information that is necessary for, or directly related to, its functions or activities. It collects information about a person in order to provide a service to them or, in the case of carer applicants, carers, job applicants and employees, to ensure that they are able to promote the welfare of the children, young people or people with disability using our services. This includes sensitive information.

CareSouth collects information in the following ways:

- sought directly from an individual client, carer or employee
- provided automatically by government agencies or other organisations as part of a referral for service
- via reference checks conducted on potential carers and employees, using the contact information provided by the applicant
- collecting employee medical information under WHS and Workers Compensation and pre-employment medical examinations
- by requesting data and records from Government or other agencies under information exchange arrangements, such as through the Carer's Register, criminal history checks and Working With Children Check
- by requesting information from other individuals or organisations involved in supporting and caring for an individual, such as schools, medical and health service providers, clinical specialists, family members and carers.

4.1.1. Anonymity and pseudonymity

The requirements of CareSouth's program/service funding agreements and its obligation to protect and care for children and vulnerable people mean that CareSouth is generally unable to offer its clients, employees and carers anonymity or use of a pseudonym.

CareSouth requires accurate identification and personal information in relation to:

- prospective and current clients — in order to assess eligibility and provide the required services
- employees, carers and volunteers — in order to process probity checks and support the protection of clients we work with.

4.1.2. Unsolicited personal information

CareSouth observes the following practices in relation to unsolicited personal information (information that CareSouth has taken no active steps to collect):

- Misdirected mail is returned unopened to sender
- Misdirected emails are deleted immediately
- Unsolicited correspondence, petitions that contains names and addresses and promotional flyers containing personal information are destroyed or de-identified as soon as practicable.

CareSouth destroys or de-identifies unsolicited personal information as soon as practicable unless it is unlawful to do so.

4.2. Consents to information collection and use

Every person about whom information is collected should be aware of CareSouth's Privacy Policy. This Privacy Policy is accessible to the public on the CareSouth website (www.caresouth.org.au) and is made available in writing to any person who requests it.

CareSouth includes Privacy Collection Notice and Consent statements on its print-based information collection forms, and provides readily accessible links to the equivalent information through its online forms.

Individuals must provide their express consent to the collection of personal information by signing or electronically confirming their acceptance of the relevant Privacy Collection Notification and Consent statement.

Each Privacy Collection Notification and Consent form includes the following information, written to specifically reflect the type of information being collected and the reason it is being collected:

- CareSouth's identity and contact details
- the reason the information is being collected, including whether the collection is required or authorised by law
- any consequences if personal information is not collected
- CareSouth's usual disclosures of personal information of the kind being collected
- a reference or link to CareSouth's Privacy Policy.

If personal information is collected by telephone, CareSouth explains the relevant Privacy Collection Notice to the individual at the commencement of the call. CareSouth provides the individual with access to a full copy of the relevant Privacy Collection Notification and Consent statement as soon as possible afterwards. This may be through a subsequent electronic or paper-based communication, or directing the individual to the relevant notice on the CareSouth's website.

4.2.1. Capacity to consent

Specific requirements around ensuring that an individual with disability has capacity to consent, or identifying who can act on the individual's behalf, are outlined in CareSouth's *DIS-014 Client Decision-Making and Consent* policy and *PRO-DIS-006 Client Decision-Making and Consent* procedure.

4.3. Use and disclosure of personal information

CareSouth protects the privacy of its clients, carers and employees by ensuring that it only uses or discloses personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies.

The exceptions include where:

- the individual has consented to a secondary use or disclosure
- the individual would reasonably expect CareSouth to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose
- the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order
- a permitted general situation exists in relation to the secondary use or disclosure

- a permitted health situation exists in relation to the secondary use or disclosure
- CareSouth reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

At no time is a child or young person in care to be identified in any written or pictorial information in the public arena, including social media.

4.3.1. Use and disclosure within CareSouth and between CareSouth entities

Personal information may be used by a number of people within CareSouth, but only by people who require this information to provide a service. Given the 24-hour nature of much of CareSouth's work, and the multiple carers and employees that can be supporting an individual at any one time, information needs to be exchanged between people on a 'need to know basis'.

This may occur when:

- more than one employee or carer is involved with a client. This reduces the likelihood of the client having to retell their story, and assists the carers, volunteers and employees involved to be more coordinated in providing services to the client.
- the carers, volunteers and employees involved need support or assistance from other employees or supervisors. This will assist the carers, volunteers and employees to provide a better service, as they may need new ideas, information and/or feedback on intended strategies.
- a family member's behaviour is affecting other service users, carers, volunteers or employees or there is significant risk. This may include violent behaviour, self-harm, suicide potential, other mental health concerns or substance abuse.
- contact is made with CareSouth's After Hours Service by a client or carer in relation to an incident, emergency or urgent request.

CareSouth's internal access controls for software systems and individual records reflect this 'need to know' approach. Employees have access to personal information relating only to clients of the service in which they work. Access permissions and restrictions are embedded in CareSouth's IT policies, based on information provided by Human Resources.

Only approved Human Resources employees and supervisors/managers of individual employees can have access to employee information.

Information access may be tracked or audited by CareSouth's IT Department in order to ensure compliance with this policy.

4.3.2. Research and reporting

Information on people using CareSouth's services is sometimes used for research purposes, to improve the situation for other children and young people. All requests to provide access to clients or their records must be approved first by the Manager, Policy and Research, and then by the applicable Regional Manager.

CareSouth may also be required to provide information to funding bodies such as government departments as part of its contractual reporting and data provision

requirements. In these situations the funding body is responsible for de-identifying the information in accordance with its own de-identification protocols.

4.3.3. Government-related identifiers

CareSouth routinely collects information about individuals that includes Government identifiers (such as an individual's Medicare number, Driver's Licence number, Tax File Number or Centrelink Customer Reference Number) as part of its work with clients.

These identifiers are recorded in CareSouth's files, but are not used as an identifier for the individual or family at any time, i.e. files are not labelled or organised using any of these identifiers as naming conventions.

CareSouth does not use any government-related identifier to identify individuals except where it is required to do so by law.

CareSouth does not use or disclose the government-related identifier of an individual except:

- where the use or disclosure is necessary to verify the identity of the individual in order to provide services, or for employment or authorisation as a carer
- where use or disclosure is necessary to fulfil its obligations to a Commonwealth or a State or Territory agency
- as required or authorised by or under an Australian law or a court/tribunal order.

4.4. Exchange of personal information with third parties

CareSouth collects and discloses information with third parties in line with its responsibilities under legislation.

4.4.1. Exchange of information with other 'prescribed bodies'

CareSouth has an obligation to exchange information with other agencies which may assist in protecting CareSouth clients and other vulnerable members of the community. This obligation is entrenched in Chapter 16A and s248 of the *Children and Young Persons (Care and Protection) Act 1998 (NSW).*

CareSouth frequently obtains information from sources other than the person directly accessing our services. This includes information obtained from the body that refers a client to CareSouth, such as FACS, and specific situations where. CareSouth is required to obtain information from a secondary 'entity'. Examples include information on court orders in place for a child and other information required in order to provide safe and appropriate service.

CareSouth also has legal obligations to provide information to other 'prescribed bodies' (usually other welfare agencies), which may request information in order to promote the safety, welfare and wellbeing of children and young people.

CareSouth's process for exchanging information with other agencies is detailed in the *ORG-REC-006 Exchange of Information* policy and *PRO-ORG-REC-006 Exchange of Information* procedure.

In some cases, employee information may be provided to solicitors and other organisations for the purposes of Workers Compensation claims and legal

proceedings. This exchange will be conducted in accordance with Human Resources and Workplace Health and Safety policies and procedures.

4.4.2. Providing information to a Court

When asked to submit information to a Court, CareSouth will only do so when issued with a subpoena or with the permission of the person involved. Note that it is possible to challenge the amount of information required in a subpoena as outlined in CareSouth's *ORG-REC-003 Subpoena Compliance* policy and *PRO--ORG-REC-003 Subpoena* procedure.

4.4.3. Carer applicants and carers

CareSouth obtains personal information from prospective carers and others residing on their premises during the carer assessment process. This information is used to assess the applicant's suitability for authorisation as a carer.

The carer assessment process is a structured process involving written information, training, structured interviews, medical and probity checks, and includes collecting the opinions of referees about an applicant.

All carer applicants and those residing on their property are subject to mandatory probity checks, which involve accessing government information through the National Criminal Record Check, Working with Children Check (NSW), Working with Vulnerable Persons (ACT), and through the Carer Register and the Community Services check for carer applicants in NSW. This may mean that both the government agency supplying the information and CareSouth will examine criminal or juvenile justice offences from the past.

Prior to any reference, health, probity or other recruitment-related checks being carried out, CareSouth requires the individuals involved to review and sign the relevant CareSouth *Privacy Collection Notification and Consent* form. This document clearly outlines the purpose and confidential storage of the applicant's information and their rights to access.

The Children and Young Persons (Care and Protection) Act 1998 defines what information can be disclosed about foster carers to birth parents. CareSouth's *OOHC-007 Disclosure of Placement Information* policy details the process for disclosing information on placements and carers to birth parents and other significant persons.

CareSouth also has a legal obligation to disclose some information about carers and carer applicants to other 'prescribed bodies'. Information on carers and carer applicants may be made available to other designated agencies when they put in a formal request.

4.4.4. Recruitment of employees

CareSouth obtains personal information from applicants during the employee recruitment process. This information is used to assess the applicant's suitability for employment with CareSouth.

As part of this process, CareSouth also collects the opinions of others about an applicant; these may relate to the applicant's experience and qualifications, work history and performance, tests or assessments (including medical tests and assessments), and other information required in connection with their application.

CareSouth also conducts mandatory probity checks on all employment and carer applicants, which involves accessing government information through the National Criminal Record Check, Working with Children Check (NSW) and Working with Vulnerable Persons (ACT).

Prior to any reference, probity or other recruitment-related checks being carried out, CareSouth requires the identified applicant to consider and sign the relevant CareSouth *Privacy Collection Notification and Consent Form*. This document clearly outlines the purpose and confidential storage of the applicant's information and their rights to access.

4.5. Marketing

CareSouth never shares or discloses personal information on its clients, carers or employees to any third party for the purposes of direct marketing.

CareSouth maintains a Client Relationship Management database with the contact details of individuals who have enquired about volunteering, becoming a carer or donating to CareSouth. This is used to evaluate the success of our engagement with applicants. Information is not distributed to those on the database, except in direct response to their request for information or a decision to subscribe to a particular information service. Any individual may request removal from the database at any time via email or telephone call.

4.5.1. Direct marketing via cookies

CareSouth uses cookies on its website. A cookie is a small piece of data that a website asks a website visitor's browser to store on their computer or mobile device and allows the website to "remember" the user's actions or preferences over time. CareSouth uses cookies to identify how users interact with content on the website and to improve user experience. It may use cookies to serve users with targeted advertisements on third-party websites.

CareSouth does not use cookies to identify individual users, or to create a profile of their browsing behaviour on third-party sites.

4.6. Cross-border disclosure of personal information

No employee will disclose any information about any individual outside Australian borders.

The only exceptions to this are:

- where the individual gives consent, or
- the issue of child protection overrides all other concerns, or
- it is legally mandated and the CEO approves its transmission, and
- a secure method of transferring the information is identified.

4.6.1. Externally-hosted storage

Some information systems used by CareSouth hold personal records electronically in cloud-based systems, which may be hosted outside Australia. Where these hold personal information, they can only be accessed with a secure password and subject to the system vendor's privacy policies.

CareSouth remains accountable for any privacy breaches if an overseas recipient mishandles the information.

Prior to adopting an information system, CareSouth ensures that:

- the system is subject to a binding agreement between CareSouth and the system vendor that ensures the vendor handles the personal information for limited purposes and in accordance with the APPs. In particular, CareSouth will assess the adequacy of the system against the following criteria:
    - CareSouth retains the right or power to access, change or retrieve the personal information
    - the personal information can be retrieved or permanently deleted by CareSouth when no longer required or at the end of the agreement
    - there are clear and appropriate restrictions on who will be able to access the personal information and for what purposes
    - security measures to be used for the storage and management of the personal information meet industry requirements.
- the agreement requires any subcontractors to agree to the same obligations
- the agreement gives CareSouth effective control of how the personal information is handled by the overseas recipient.

4.7. Access restrictions and security of personal information

CareSouth protects personal information from misuse, loss, unauthorised access, modification or disclosure at all times. Security practices and employee file access are monitored in regular scheduled audits to ensure compliance with policies.

CareSouth's measures to maintain the security of personal information include the following.

4.7.1. Physical file security

- Physical access to CareSouth premises that hold personal information is controlled by electronic keys and personal alarm access codes, available only to authorised persons.
- Filing cabinets, offices and file rooms containing personal information are locked when not in use, and keys are held only by relevant authorised employees.
- Files containing personal information are filed away when not in use, and are never to be left on desks or in areas where other people can read or access them.
- Case files, in general, should not be transported between offices unless unavoidable, and reasonable measures should be taken to ensure security.
- Appointment diaries, client contact details and notebooks containing client information are kept separately and securely, not left unattended in any public place, in a locked car etc.

4.7.2. ICT security

CareSouth has a set of ICT security processes in place to restrict access and protect personal information stored in data systems from unauthorised access, use, modification and disclosure. These are outlined in the *ORG-IT-001 Information Technology Security* Policy.

4.7.3. Work practices

- Client information is not discussed where others can overhear the conversation (in reception areas, in hallways, in the kitchen, in public areas, etc.).
- It is not acceptable to discuss client information in public areas even if the client's name is not used.
- Callers or visitors seeking to access personal information are required to verify their identity.
- When leaving a message for clients, either on an answering machine or with another person, CareSouth employees provide only their first name and the contact telephone number, and do not identify that they are calling from CareSouth.
- All confidential information is disposed of securely e.g. placed in the security bin for safe destruction.

Information on the responsibilities of employees to maintain privacy and confidentiality of all client and employee information is included in CareSouth's employee induction process and as part of the CareSouth *Code of Conduct*.

4.7.4. Destruction and de-identification

Records containing personal information may be destroyed or de-identified only in accordance with the *ORG-REC-002 Records Management Policy*, and only in cases where:

- CareSouth no longer needs the information for any purpose
- the information is not contained in a Commonwealth record
- CareSouth is not required by or under an Australian law, or a court/tribunal order, to retain the information.

4.7.5. Data breaches

Processes to be followed in the event of a data breach are outlined in the *ORG-IT-001 Information Technology Security* policy.

4.8. Quality of personal information

Any employee who collects personal information from an individual is required to make sure that the information remains current, accurate and complete throughout the time that person is using CareSouth services.

CareSouth may record opinions as part of the personal information it collects. Where an opinion about an individual is recorded, it is to:

- be presented as an opinion and not objective fact
- accurately record the view held by the third party
- be an informed assessment that takes into account competing facts and views.

CareSouth conducts regular reviews of the quality of personal information it holds as part of the case management process. This assists in ensuring it is accurate, up-to-date, complete and relevant at the time it is used or disclosed.

4.9. Client and family member access to personal information

Where CareSouth holds personal information, the person named in the file generally has the legal right to access that information. This right includes the right of a legal guardian to access personal information held by CareSouth pertaining to a child.

Children, young people, relevant family members, carers or volunteers can request access to their file at any time and CareSouth will provide that access at no cost, subject to the exceptions and restrictions outlined under 4.10.1 and 4.10.2 below. Each person has rights to the information regardless of their age, as long as they can demonstrate an understanding of the concepts of consent, personal information and privacy.

This right to access personal information is balanced against CareSouth's legislative duty to protect the information in the client file.

Carers and carer applicants also have the right to review material on the Carers Register managed by the Office of the Children's Guardian.

CareSouth manages all requests for access to personal information in accordance with *ORG-REC-008 Client Access to Records* policy and *PRO-ORG-REC-008 Client Access to Records* procedure.

4.10. Correction of personal information

CareSouth clients have the right to request and seek correction of their personal information. These requests are managed in accordance with the policy and *PRO-ORG-REC-008 Client Access to Records* procedure.

4.11. Privacy complaints

Individuals are able to make complaints about a breach of the Australian Privacy Principles to CareSouth and/or external agencies such as the Office of the Australian Information Commissioner (OAIC).

All complaints are to be managed in accordance with CareSouth's *Complaints and Feedback* procedure.

5. RESPONSIBILITIES

5.1. Employees, Volunteers, Students, Contractors, Consultants

All employees, volunteers, students, contractors and consultants carrying out work for or on behalf of CareSouth are expected to:

- observe all CareSouth requirements around privacy and confidentiality as outlined in this policy
- ensure that all clients' personal information remains current, accurate and complete throughout the time that person is using CareSouth services
- ensure that updated or new personal information is promptly added to relevant existing records
- assist with third-party requests for information exchange as required
- assist with requests for client access to personal information as required.

5.2. Managers

All Managers across CareSouth are required to:

- monitor employees to ensure that all CareSouth requirements around privacy and confidentiality are observed
- provide appropriate levels of training, coaching and supervision to ensure employees meet their responsibilities in relation to privacy and confidentiality
- foster and support a culture within their team that promotes sound privacy and confidentiality practices
- review and authorise third-party requests for information exchange
- review and authorise client or employee access to their files as required.

6. AUTHORITY

This Policy is authorised by the Chief Executive Officer.

CareSouth retains the right to amend or vary this policy, in its absolute discretion, from time to time as deemed fit.

Employees and external parties who are affected will be apprised of such changes at the time of revised publication.

7. VERSION CONTROL AND CHANGE HISTORY

Version Number	Approval Date	Approved by	Amendment
1.0	16/02/2012	CEO	Replaces 2.3 Privacy Policy
2.0	03/03/2017	CEO	Update to new policy template and inclusion of policy code and codes for associated forms. Complete revision of content to align to updated legislation and National Privacy Principles.