

Privacy Policy

How we collect, use, store and protect your personal and sensitive information, and how you can exercise your privacy rights.



Your privacy matters to us

This document sets out how Contract Care handles the personal and sensitive information you share with us. It explains what we collect, how we use and disclose it, how we keep it secure, and how you can access, correct or complain about the information we hold. It also explains how we ask for, record and respect your consent, particularly for health and other sensitive information. If you have any questions after reading this policy, please get in touch using the contact details in section 18.

This policy is written to be read alongside our Client Privacy Consent Form (Schedule 1), our Client Handbook and our Workforce Privacy Notice. Easy Read and translated versions of this policy are available on request.

1 Introduction

This document sets out the privacy policy of Contract Care OS Pty Ltd (ABN 60 679 907 674) and each of its related bodies corporate that provide care, nursing, support or workforce services under the Contract Care name, including Contract Care Services Pty Ltd (ABN 72 694 101 687), Contract Care Workforce Services Pty Ltd (ABN 40 694 100 680), Contract Care Support Services Pty Ltd (ABN 66 674 203 573) and Contract Care Group Pty Ltd (ABN 44 675 973 805) (together, Contract Care) (referred to in this privacy policy as 'we', 'us', or 'our').

We take our privacy obligations seriously and we've created this privacy policy to explain how we collect, store, maintain, use and disclose personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs), the Health Records and Information Privacy Act 2002 (NSW) and equivalent State and Territory health records laws, the National Disability Insurance Scheme Act 2013 (Cth) and the NDIS Practice Standards and Code of Conduct, and, where we deliver aged care services, the aged care legislation that applies to us.

This policy is not a consent form. Where the law requires your consent (for example, before we collect your health information), we will ask for it separately and expressly, in the way described in section 5. Nothing in this policy limits any right you have under privacy or health records law.

We may change this privacy policy from time to time by posting an updated copy on our website and, where the change materially affects how we handle your information, by telling you directly (for example by email or through your support worker or nominee). The current version is always available at contractcare.com.au and free of charge in hard copy on request.

2 Who this policy applies to

This policy applies to personal information we handle about:

- (a) clients and participants who receive (or enquire about) nursing, disability support, aged care or other care services from us, including NDIS participants (clients);

- (b)** family members, carers, guardians, nominees, support coordinators, plan managers and other representatives of our clients;
- (c)** our workforce – employees (including casual nurses and care staff), contractors, agency workers, volunteers and students on placement – and people who apply to work with us;
- (d)** referrers, health practitioners, suppliers, investors and other business contacts; and
- (e)** visitors to our website and social media pages.

Some of our handling of current and former employee records is exempt from the APPs under the employee records exemption. We nevertheless handle all workforce information in accordance with this policy as a matter of good practice, and our obligations under the NDIS worker screening and Fair Work record-keeping rules continue to apply.

3 Types of personal information we collect

The personal information we collect depends on your relationship with us and may include the following:

- (a)** name;
- (b)** mailing or street address;
- (c)** email address;
- (d)** social media information;
- (e)** telephone number and other contact details;
- (f)** age;
- (g)** date of birth;
- (h)** passport details, visa and right-to-work details;
- (i)** other identification documents, including but not limited to driver's licences;
- (j)** details relating to police checks, NDIS Worker Screening Checks and Working With Children Checks;
- (k)** details about your qualifications, professional registration (including AHPRA registration number and status) and training certificates;
- (l)** credit card, bank account or other payment information;
- (m)** sensitive information (such as health information) as set out in section 9;
- (n)** information about your business or personal circumstances, living arrangements and support needs;
- (o)** information in connection with client surveys, questionnaires and promotions;
- (p)** your device identity and type, I.P. address, geo-location information, page view statistics, advertising data and standard web log information;
- (q)** information about third parties (such as your emergency contacts, next of kin or nominee); and
- (r)** any other information provided by you to us via our website or our online presence, or otherwise required by us or provided by you.

If you are a client, we may also collect

- (s)** your NDIS participant number, plan details, plan goals, funding and budget information, and the details of your plan manager, support coordinator and nominee;
- (t)** care and support plans, risk assessments, progress notes, shift notes, medication charts, observations and clinical records made by our nurses and support workers;
- (u)** incident, complaint and feedback records, including records we are required to keep or report under the NDIS Practice Standards and reportable incident rules;
- (v)** your preferences about how services are delivered, including language, cultural and communication needs; and
- (w)** details of other providers, health practitioners and services involved in your care.

If you work or apply to work with us, we may also collect

- (x)** your employment history, references and referee contact details, résumé and interview records;
- (y)** tax file number, superannuation fund, bank account and payroll details (collected only after an offer of employment);
- (z)** immunisation and vaccination evidence required for placement with clients, and fitness-for-work information where relevant to your role;
- (aa)** rostering, timesheet, location check-in and shift data from our rostering and care management systems;
- (bb)** performance, training, supervision, incident and disciplinary records; and
- (cc)** emergency contact details.

If you choose not to give us information we ask for, we may not be able to provide services to you, consider your application, or deal with you effectively. We will tell you if this is the case.

4 How personal information is collected

We will collect your personal information in a lawful and fair way and, wherever reasonable and practicable, directly from you. We will only collect sensitive information (including health information) where you have consented to it (see section 5), or otherwise where the law permits or requires us to. We will only collect other personal information where it is reasonably necessary for one or more of our functions or activities.

How we collect information from you

We may collect personal information where you:

- (a)** contact us through our website;
- (b)** receive goods or services from us, including during intake, assessment, care planning and service delivery;
- (c)** submit any of our online enquiry forms;
- (d)** communicate with us via email, telephone, SMS, social applications (such as LinkedIn or Facebook) or otherwise;

- (e) interact with our website, social applications, services, content and advertising;
- (f) invest in our business or enquire as to a potential purchase in our business;
- (g) apply for a role with us, complete onboarding, or work with us; and
- (h) give us feedback or make a complaint.

How we collect information from third parties

Where possible, we collect your personal information directly from you. However, there may be occasions when we collect personal information (including sensitive information) about you from someone else. For example, from a parent or guardian (where you are under the age of 18 years, and we determine that you do not have the capacity to consent), your nominee, guardian or support coordinator, the National Disability Insurance Agency (NDIA), a hospital, GP or allied health professional involved in your care, an aged care assessment service, or where we receive a referral for our services from another health care provider. For workforce members, we may collect information from referees, AHPRA, worker screening units, police check providers, visa verification services and training providers.

If we receive personal information we did not ask for and could not lawfully have collected, we will destroy or de-identify it as soon as practicable, where it is lawful and reasonable to do so.

How you provide information for someone else

If you are providing personal and/or sensitive information on behalf of someone else, you must have the authority or consent of that person to provide their personal and/or sensitive information to us to be collected, used, and disclosed in accordance with this privacy policy. This includes where you are a NDIS participant's nominee, support coordinator, plan manager, guardian, enduring attorney or representative. We reserve the right to request evidence of this authority or consent (such as a nominee appointment, guardianship order or enduring power of attorney).

If you are providing personal and/or sensitive information on behalf of someone under the age of 18 (Minor), you must be that Minor's parent or legal guardian and you must provide consent for the Minor's personal and/or sensitive information to be collected, used and disclosed in accordance with this privacy policy and the consent process in section 5. Where a young person has the capacity to make their own decisions, we will seek their consent and involve them in decisions about their information.

How we collect information from cookies

We may also collect personal information from you when you use or access our website or our social media pages. This may be done through use of web analytics tools, 'cookies' or other similar tracking technologies that allow us to track and analyse your website usage. Cookies are small files that store information on your computer, mobile phone or other device and enable and allow the creator of the cookie to identify when you visit different websites. If you do not wish information to be stored as a cookie, you can disable cookies in your web browser.

5 How we obtain and record your consent

We rely on your express consent before we collect, use or disclose your sensitive information (including health information), unless an exception under privacy law applies. This section describes the process we follow.

When we ask for your consent

- (a)** Before or at your first appointment, assessment or service, and before we collect your health information from you or from a referrer, we will ask you to complete our Client Privacy Consent Form (a copy is at Schedule 1).
- (b)** We will ask again if we want to use or disclose your sensitive information for a new purpose that you would not reasonably expect, or to a new type of recipient not covered by your original consent.
- (c)** We will review your consent with you at each care plan or NDIS plan review, and at least every 12 months, and ask you to confirm or update it.

How we ask

- (d)** We explain, in plain language, what information we will collect, why we need it, who we will share it with, how long we keep it, and that you can say no or change your mind. We answer any questions before you decide.
- (e)** We will provide the information in a way you can understand, including Easy Read or translated formats, an interpreter, or verbal explanation, and we allow time for you to consider it and to involve a trusted person if you wish.
- (f)** Consent must be given voluntarily. We will never make consent to non-essential uses (such as marketing, testimonials or photographs) a condition of receiving services.
- (g)** Consent is specific. Our consent form lets you agree to some uses and not others, and we will record exactly what you have and have not agreed to.

Capacity and supported decision-making

- (h)** We presume that every adult has the capacity to make decisions about their own information. Where there are reasonable grounds to believe you may need support to make the decision, we will offer support (for example involving a trusted person, using accessible formats or breaking the decision into steps) before concluding that you cannot consent.
- (i)** Where you do not have the capacity to consent, we will seek consent from your authorised representative (such as an NDIS nominee, guardian or person responsible under State or Territory law) and record the basis of their authority. We will still involve you as far as possible and respect your expressed wishes.

How we record consent

- (j)** Your signed (or verbally given and witnessed) consent is stored on your client file in our care management system, together with the date, the person who obtained it, the version of this policy and the consent form in force at the time, and any limits you placed on it.
- (k)** We maintain a consent register so we can see, before disclosing your information, whether we hold current consent for that disclosure.

- (l) Verbal consent is only relied on where it is not practicable to obtain written consent (for example an urgent service change). It is recorded in your file at the time and confirmed in writing as soon as practicable.

Withdrawing consent

- (m) You can withdraw or change your consent at any time by telling your support worker or nurse, or by contacting our Privacy Officer using the details in section 18. We will act on your request as soon as practicable, update your file and consent register, and confirm the change with you.
- (n) Withdrawing consent does not affect uses or disclosures that happened before you withdrew it. If withdrawing consent means we can no longer safely or lawfully provide a service, we will explain this to you and discuss your options.

When we may act without consent

We may collect, use or disclose your sensitive information without consent only where privacy law permits, for example where it is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety and it is unreasonable or impracticable to obtain consent; where it is required or authorised by law (including mandatory reporting and reportable incident obligations); or where a permitted health situation applies. We keep a record of any such collection, use or disclosure.

6 Use of your personal information

We collect and use personal information for the following primary purposes:

- (a) to provide goods, services or information to you, including assessing your needs, planning and delivering your care and supports, and coordinating with your other providers;
- (b) for record keeping and administrative purposes;
- (c) to provide information about you to our contractors, employees, consultants, agents or other third parties for the purpose of providing goods or services to you;
- (d) to improve and optimise our service offering and customer experience;
- (e) to comply with our legal obligations, resolve disputes or enforce our agreements with third parties, including our obligations under the NDIS Practice Standards, Code of Conduct and reportable incident and complaints rules;
- (f) to send you administrative messages, reminders, notices, updates, security alerts, and other information requested by you;
- (g) to consider an application of employment from you and, if you work with us, to manage your engagement, rostering, payroll, worker screening, training, supervision, work health and safety and performance;
- (h) to claim payment for services from the NDIA, plan managers, Services Australia, private health insurers or you; and
- (i) to conduct quality, safety and clinical governance activities, including audits, incident reviews and accreditation.

We may also use your personal information for:

- (j)** secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use (for sensitive information, the secondary purpose must be directly related to the primary purpose);
- (k)** such purposes where we reasonably believe that use of your personal information is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety, and it is unreasonable or impracticable to obtain your consent;
- (l)** any other purpose for which we receive consent from you; or
- (m)** any other purpose which is permitted or required under applicable privacy laws.

Automated decision-making

We use approved computer programs at times to make, or to do something substantially and directly related to making, decisions that could reasonably be expected to affect your rights or interests. A person reviews any decision of this kind before it takes effect, and you can ask us how a decision about you was made, ask for it to be reviewed by a person, or make a complaint under section 17.

7 How we disclose your personal information

We respect your privacy, and we will take reasonable steps to keep your personal information confidential and protected. We do not sell personal information. We may disclose your personal information to:

- (a)** other health care providers we refer you to or from who we receive a referral for you, and other members of your care team (such as your GP, specialists, allied health providers, pharmacy and hospital) where this is needed for your care;
- (b)** the NDIA, the NDIS Quality and Safeguards Commission, and your plan manager, support coordinator and nominee (if applicable);
- (c)** our professional advisors such as lawyers, accountants and auditors;
- (d)** our related entities within Contract Care, so that we can manage our workforce, services and systems as one group;
- (e)** any third parties you have consented personal information to be disclosed to;
- (f)** government agencies, regulators and bodies such as Services Australia, State and Territory health and community services departments, worker screening units, AHPRA and the Aged Care Quality and Safety Commission, where required or authorised by law;
- (g)** our insurers, workers compensation insurers and, where relevant, our funders and investors' advisers (on a confidential and, wherever possible, de-identified basis); and
- (h)** for workforce members: our clients and their families (limited to your name, role, qualifications, screening status and photo where needed for the service), payroll and superannuation providers, the Australian Taxation Office and visa sponsorship authorities.

We may also disclose personal information to third party contractors as required for us to provide our goods and services to you, such as cloud-service providers, IT professionals, care management, rostering and payroll software providers, marketing agencies and debt collection agencies.

We take care to work with such third parties who we believe maintain an acceptable standard of data security and require them by contract not to use your personal information for any purpose except for those activities we have asked them to perform on our behalf.

We will not otherwise disclose your personal information unless:

- (i)** you have consented to us disclosing your personal information for particular circumstances;
- (j)** as needed in an emergency or in the investigation of suspected criminal activity;
- (k)** we are required to disclose under a subpoena, court order or other mandatory reporting requirements;
- (l)** we reasonably believe that disclosure of your information is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety, and it is unreasonable or impracticable to obtain your consent;
- (m)** it is reasonably necessary for the establishment, exercise or defence of a legal claim; or
- (n)** it is otherwise authorised or required by law.

8 Storage of your personal information and overseas disclosure

All personal information we collect is stored on servers located in Australia and, for the most part, we do not disclose or transfer personal information overseas.

We also may use Google Analytics to track web traffic information which is operated by Google which stores information across multiple countries.

When you communicate with us through a social media service such as Facebook or X (formerly Twitter), Instagram or LinkedIn, the social media provider and its partners may collect and hold your personal information overseas.

Before we disclose personal information to an overseas recipient, we take reasonable steps to ensure the recipient handles it in a way that is consistent with the APPs, or we obtain your consent to the disclosure. Other than the storage and support arrangements described above, we do not send your health information overseas for the purpose of delivering your care.

9 Sensitive information

Collection of sensitive information

We may collect sensitive information about you during the course of providing you our goods and services, or in the course of your work with us. We will only collect this sensitive information where you consent to such collection in the way described in section 5 and either directly provide us with this information or it is provided by a referring health care provider or your authorised representative, or where the law otherwise permits or requires us to collect it.

Types of sensitive information we collect

The sensitive information we collect may include the following:

- (a) health information, history and reports, including diagnoses, medications, allergies, disability and functional assessments, mental health information, behaviour support plans and records relating to the use of restrictive practices;
- (b) reports about your vaccination history, including COVID-19 vaccinations;
- (c) referring health care provider and associated referral documents;
- (d) your NDIS participant details, plan goals and management of funding for goods and services;
- (e) private health fund and private health insurance cover details;
- (f) Medicare number, healthcare identifiers or concession card or other entitlement details;
- (g) any other sensitive information provided by you or a third party to us via our website or platforms, or otherwise provided by you or a third party to us;
- (h) information about your cultural background, Aboriginal or Torres Strait Islander status, language, religious or spiritual beliefs and sexual orientation or gender identity, only where you choose to share it and it is relevant to delivering culturally safe and appropriate care; and
- (i) for workforce members and applicants: criminal history information contained in police checks and NDIS Worker Screening or Working With Children Check outcomes, professional registration conditions, and health information relevant to your fitness for work or a workplace injury.

How we use your sensitive information

Your sensitive information will only be used for the purpose of:

- (j) providing you with our goods and services, including planning, delivering, reviewing and claiming payment for your care and supports;
- (k) complying with our legal obligations, resolving disputes or enforcing our agreements with you;
- (l) sending you messages, reminders, notices, updates, security alerts, and other information requested by you;
- (m) for workforce members, assessing your suitability to work with vulnerable people and meeting our worker screening, safety and clinical governance obligations; or
- (n) any other purpose which is permitted or required under applicable privacy laws.

We do not use sensitive information for direct marketing without your express consent.

How we disclose your sensitive information

Your sensitive information will only be disclosed to third parties with your consent or as otherwise permitted by law, and for the purpose of:

- (a) providing you with services (and other related purposes, for example liaising with other support providers, your nominee or your plan manager);
- (b) providing a referral to a health care provider; or
- (c) any other purpose which is permitted or required under applicable privacy laws.

How you can withdraw consent

If you wish to withdraw your consent to our collection, use or disclosure of your sensitive information, please contact us using the contact details set out below or speak with your support worker or nurse. We will deal with all such requests as described in section 5.

10 Government identifiers

We collect government-related identifiers such as your Medicare number, NDIS participant number, healthcare identifier or (for workforce members) tax file number only where this is required or authorised by law or is reasonably necessary to verify your identity or to claim funding for your services. We do not adopt these identifiers as our own identifier for you, and we use and disclose them only for the purpose for which they were collected.

11 Marketing

We may at times send you marketing communications which will be done in accordance with the Spam Act 2003 (Cth) (Spam Act) and the Do Not Call Register Act 2006 (Cth).

If we do, we may use email, SMS, social media, phone or mail to send you direct marketing communications.

Where consent is needed, we will ask you for your consent before sending you marketing communications, except where you:

- (a) have explicitly opted-in to receiving email marketing from us in the past; or
- (b) were given the option to opt-out of email marketing when you initially signed up for one of our platforms and you did not do so.

You can, at any time, opt out of receiving marketing materials from us by using the opt-out facility provided (e.g., an unsubscribe link on emails we send you) or by contacting us via the details provided at the end of this privacy policy. We will implement such a request as soon as possible and in any event within 5 business days, however, cannot guarantee that such a response will be immediate. We will not use your sensitive information for marketing, and we will not use your image, story or testimonial in marketing, without your separate express consent, which you can withdraw at any time.

12 De-identified information

The information we collect may have analytical, educational, or commercial value to us. Where we have de-identified the information we have collected so that you can no longer reasonably be identified, we may process and share such information, for example for service planning, quality improvement, reporting to funders and investors, and research. We will seek your consent before releasing any case study or written material that describes your circumstances, even where your name has been removed.

13 Security, data quality, retention and destruction

We take reasonable steps to ensure your personal information is accurate, up to date and complete, and is secure and protected from misuse, interference, loss or unauthorised access, modification or disclosure. Our information technology systems are password protected, and we use a range of administrative and technical measures to protect these systems, including multi-factor authentication, role-based access so that staff only see the client information they need for their role, encryption of data in transit and at rest on our core platforms, audit logs, secure disposal of paper records, and privacy and information-security training for all staff at induction and annually. Physical records are kept in locked storage. However, we cannot guarantee the security of your personal information.

How long we keep your information

We keep personal information only for as long as we need it for the purposes described in this policy or as required by law. In particular:

- (a)** client care records (including health information) are kept for at least 7 years from the date of the last entry or service or, if you were under 18 when the record was made, until you turn 25, whichever is later, consistent with the NDIS Practice Standards and State and Territory health records laws;
- (b)** incident, complaint and restrictive practice records are kept for at least 7 years;
- (c)** employee and payroll records are kept for at least 7 years after employment ends, as required by the Fair Work Act 2009 (Cth); and
- (d)** unsuccessful job applications are kept for up to 12 months unless you ask us to keep them longer.

When we no longer need personal information and are no longer required to keep it, we take reasonable steps to destroy it securely or permanently de-identify it.

14 Data breaches

We have a data breach response plan. Where we have reasonable grounds to suspect an eligible data breach, we will complete our assessment expeditiously and in any event within 30 days of becoming aware of the grounds for suspicion. If we become aware of a suspected data breach involving your personal information, we will contain it, assess it and take steps to reduce any harm. If the breach is likely to result in serious harm to you, we will notify you and the Office of the Australian Information Commissioner (OAIC) as required by the Notifiable Data Breaches scheme in the Privacy Act 1988 (Cth), and tell you what you can do to protect yourself. Where a breach is also a reportable incident under the NDIS rules, we will notify the NDIS Quality and Safeguards Commission.

15 Links

Our website may contain links to other websites. Those links are provided for convenience and may not remain current or be maintained. We are not responsible for the privacy practices of those linked websites and we suggest you review the privacy policies of those websites before using them.

16 Your rights over your personal information

You have the following rights, which you can exercise free of charge by contacting our Privacy Officer (section 18). You can also ask your support worker, nurse or nominee to help you make a request.

Dealing with us anonymously

Where it is lawful and practicable, you may deal with us anonymously or using a pseudonym, for example when making a general enquiry. We cannot provide care services or process an application anonymously.

Access

If you wish to request access to the personal information we hold about you, please contact us using the contact details set out below including your name and contact details. We may need to verify your identity before providing you with your personal information. In some cases, we may be unable to provide you with access to all your personal information (for example where giving access would pose a serious threat to someone's life, health or safety, would unreasonably affect another person's privacy, or is prevented by law) and where this occurs, we will explain why in writing and tell you how you can complain. We will deal with all requests for access to personal information within 30 days. We will give you access in the form you request where reasonable and practicable (for example a copy of your care plan or progress notes). We do not charge a fee for making a request, and any charge for giving access will be reasonable and told to you in advance.

Correction

If you think that any personal information we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, please contact us using the contact details set out below and we will take reasonable steps to ensure that it is corrected within 30 days. If we do not agree to correct it, we will tell you why in writing, and, if you ask, we will attach a statement to the record noting that you consider it inaccurate. If we correct information we have previously given to a third party, we will tell them of the correction if you ask us to and it is practicable to do so.

Other rights

You can also, at any time: withdraw or vary your consent (section 5); opt out of marketing (section 11); ask us what information we hold about you and where it came from; ask us to delete information we no longer need to keep by law; nominate a representative to deal with us on your behalf; and make a complaint (section 17). Exercising your rights will never affect the quality of care you receive from us.

17 Complaints

If you wish to complain about how we handle your personal information held by us, please contact us using the details set out below including your name and contact details. We will acknowledge your complaint within 5 business days, investigate your complaint promptly and respond to you in writing within 30 days. If we need longer, we will tell you why and when you can expect a response.

If you are not satisfied with our response, or you would prefer not to raise the matter with us, you can complain to:

- (a)** the Office of the Australian Information Commissioner (OAIC) – www.oaic.gov.au, 1300 363 992, GPO Box 5288 Sydney NSW 2001;
- (b)** the NDIS Quality and Safeguards Commission (for NDIS participants) – www.ndiscommission.gov.au, 1800 035 544;
- (c)** the Information and Privacy Commission NSW (for health information handled in NSW) – www.ipc.nsw.gov.au, 1800 472 679; or
- (d)** the Aged Care Quality and Safety Commission (for aged care services) – www.agedcarequality.gov.au, 1800 951 822.

Making a complaint will never affect the services you receive from us. You may use an advocate or support person at any stage.

18 Contact us

For further information about our privacy policy or practices, or to access or correct your personal information, to withdraw consent, or make a complaint, please contact our Privacy Officer using the details set out below:

Name	Dennis Pili-Gaitau, Privacy Officer
Email	privacy@contractcare.com.au
Phone	(02) 9052 4930
Post	Privacy Officer, Contract Care, Level 2, 383 George Street, Sydney NSW 2000

Our privacy policy was last updated on September 2026 (Version 2.0). We review this policy at least every two years and whenever our services, systems or the law change.