



PRINTED COPIES ARE NOT CONTROLLED

Policy

QUEENSLAND CHILDREN'S CLINIC P/L PRIVACY POLICY (V1) 260116

QUEENSLAND CHILDREN'S CLINIC P/L PRIVACY POLICY

Here at Queensland Children's Clinic Pty Ltd ACN: 646 526 061 (**we, us** or **our**), protecting your privacy and treating your personal information in accordance with Australian privacy laws is of paramount importance to us. This Privacy Policy explains what personal information we collect, why we collect personal information and how we collect, use, disclose, store and protect your personal information when you visit our website (**Website**), use our paediatric, nurse practitioner and allied health services, or continue to use our services (**Services**). This Privacy Policy also applies to independent contractors who deliver services under our systems and to our third-party IT providers, who manage our email and security infrastructure. As a healthcare provider, we are committed to maintaining the highest standards of privacy protection for sensitive health information.

Our Privacy Policy also explains how to contact us to correct, update or delete any personal information provided to us, or make a complaint if you have concerns. We are compliant with the *Privacy Act 1988* (Cth) (**Privacy Act**) and the Australian Privacy Principles (**APPs**).

We maintain secure records of all user consents and withdrawals to ensure compliance with data protection regulations and to respect your privacy choices. These records are kept for the duration of our relationship with you and for a reasonable period thereafter as required by applicable laws.

Unless otherwise indicated by the context, words importing the singular include the plural and vice versa.

CHANGES THAT WE MAKE TO OUR PRIVACY POLICY

We will notify you about any changes to our Privacy Policy by updating the "Last Updated" date of this Privacy Policy and posting the updated version on our Website. You are encouraged to periodically review this Privacy Policy to stay informed of updates. We will seek your consent for any changes in our Privacy Policy that affect how we process your personal information, particularly regarding sensitive health information or changes to our information sharing practices. If you do not agree with the changes, you may choose to stop using our services, though we will continue to protect any information previously collected in accordance with the privacy policy under which it was collected.

COLLECTION OF YOUR PERSONAL INFORMATION BY THIRD PARTIES

This Privacy Policy does not apply to any third-party service or website which we connect to, and which may also collect and use information about you. We are not responsible for the privacy practices of any third party, including but not limited to payment processors, or other healthcare practitioners who may be involved in your care. We encourage you to review the privacy policies of all third-party services you interact with through our platform.

WHICH ENTITIES DOES THIS PRIVACY POLICY COVER?

This Privacy Policy applies to us with respect to content on our website, our allied health services, and information you provide to us about yourself through any of our service delivery channels.

WHAT IS PERSONAL INFORMATION?

Personal information is defined as information, whether true or not, about an individual who can be identified:

1. from that information; or
2. from that information and other information to which the organisation has or is likely to have access.

This includes both general personal information such as your name and contact details, as well as sensitive personal information such as health records, medical history, and information about your physical and mental health.

WHEN AND HOW DO WE COLLECT YOUR PERSONAL INFORMATION?

We collect most personal information directly from you when you consent to use our Services or receive communications from us, or information we receive from third parties such as schools, educators, and other care providers involved in the child's health and development (where authorised), your treating general practitioner, specialist medical practitioners, or other health services. Your consent may be express (for example, you agree to the use of your information by completing our online intake forms when you become a patient) or implied by an action you take or do not take (such as because you have agreed to terms and conditions that contain information about the use or disclosure of your information).

You provide us your information when you use our allied health Services, complete our intake forms, communicate with our team, or you use our Website generally or you deal with us in any capacity related to your healthcare journey.

When we collect your personal information, we will take reasonable steps to notify you (or ensure you are aware) of the purposes for which we are collecting it, who we may disclose it to, and how you may access or correct it. This notification may be provided in our intake form, via our website enquiry form, or verbally during your consultation.

WHAT PERSONAL INFORMATION DO WE COLLECT?

Personal Information

We may collect and process various types of personal information, including sensitive personal information. Sensitive personal information includes information such as racial or ethnic origin, political opinions, religious beliefs, health information, or biometric information (**Sensitive Information**). When we collect Sensitive Information, we implement additional safeguards to protect this information, including enhanced security measures, stricter access controls, and specialised handling procedures in compliance with applicable laws and regulations.

We may provide Sensitive Information relating to your health to other allied health service providers, such as your general practitioner or specialist medical practitioners, and we may disclose your Sensitive Information to third party service providers whom we engage to support our clinical operations and service delivery. We will only supply this information with your consent, or in circumstances where it is required for the delivery of health services, such as referral to another health service provider, where it is necessary to prevent or lessen a serious threat to a patient's life, health or safety, or other reason as permitted by law.

We collect personal information necessary for providing our services. This includes:

Demographic and Contact Information

Your full name, date of birth, gender, pronouns, residential address, postal address, telephone numbers, email address, emergency contact details, and next of kin information as required for our service delivery and emergency contact purposes.

Government and Healthcare Identifiers

Medicare number and any relevant pension concession card details that may affect your healthcare entitlements.

Health and Medical Information

We collect Sensitive Information including your medical history, previous treatments, medications, diagnoses, disability details, treatment plans, mental health information, appointment and billing details, and future wishes about health services. This may include clinical photographs/images provided by parents/carers (for example, images emailed to us for clinical purposes) stored in the patient record. We may also use secure clinical dictation tools (currently Heidi) which create audio recordings and/or transcripts as part of clinical note-taking and record keeping.

Third-Party Medical Information

We collect information from third parties with your consent, including GPs, hospitals, NDIS coordinators, and family members. This may include transfer of notes from other GP clinics, discharge information from hospitals, and specialist letters.

Health and Medical Information

We may also collect clinical photographs or images provided by parents/carers (for example, images emailed to us for clinical purposes) which are stored in the patient record. We may use secure clinical dictation tools which create voice recordings or transcriptions as part of clinical note-taking.

Collection Methods

Our practice employs digital and paper-based collection methods. We collect personal information directly from clients through intake forms and during consultations. We may also collect information from third parties such as general practitioners, specialists, or other health professionals involved in the client's care. Disclosure to third parties will generally occur with the client's consent, which may be documented via email authorisation saved in the client's file or a note if verbal consent is given. This consent is typically obtained via our New Patient consent documentation, which is scanned into the patient file, and may also be recorded in consultation notes where verbal consent is provided.

You can choose not to provide us with your personal information. However, please note that if you do not provide this information, you may not be able to take full advantage of some of the features of our services. It is important to note that the provision of personal information is voluntary. You have the right to withdraw your consent at any time, in which case you should contact us using the contact details provided in this policy. However, withdrawal of consent may impact our ability to provide certain services, particularly those requiring comprehensive medical information for safe and effective care delivery.

WHY DO WE COLLECT YOUR PERSONAL INFORMATION?

We may collect your personal information when required by law but generally we collect personal information from you (or about you) to allow us to provide you with our services, for care planning, billing, compliance reporting, quality improvement, research, training, and to ensure your experience with us is positive, safe, and therapeutically beneficial.

Personal information collected or received by us will only be used for the stated purpose for which it was provided, or for purposes that are directly related to the primary purpose of collection and would be reasonably expected by you in the circumstances.

We may also use de-identified information for quality assurance, staff training, and administrative purposes.

WHEN DO WE DISCLOSE YOUR PERSONAL INFORMATION?

We may collect, hold, use and disclose your personal information for the following purposes:

- to enable you to access and use our services;

- to operate, protect, improve and optimise our services, business operations and our patients' experience, such as to perform clinical quality assessments;
- to send you service, support and administrative messages, reminders, technical notices, updates, security alerts, and information requested by you; and
- to comply with our legal obligations, resolve any disputes that we may have with any of our users, and enforce our agreements with third parties.

This third party may combine that information in order to enable it and us to develop anonymised consumer insights so that we can better understand your preferences and interests, personalise your experience and enhance the products and services that you receive.

We may disclose personal information for the purposes described in this privacy policy to:

- treating practitioners and referrers;
- hospitals;
- government agencies including Medicare and the NDIA;
- NDIS related providers;
- our employees and related bodies corporate;
- third party suppliers and service providers (including providers for the operation of our websites and/or our business or in connection with providing our products and services to you);
- payment systems operators (eg merchants receiving card payments);
- anyone to whom our assets or businesses (or any part of them) are transferred;
- specific third parties authorised by you to receive information held by us; and
- other persons, including government agencies, regulatory bodies and law enforcement agencies, or as required, authorised or permitted by law.

We maintain strict consent protocols for all information sharing, recognising the sensitive nature of health information and the importance of maintaining patient confidentiality while ensuring comprehensive care coordination.

Third-Party Information Sources and Healthcare Provider Relationships

Our practice receives information from various third-party sources essential for providing our services. We maintain consent protocols for all third-party information sharing, recognising the importance of care coordination while protecting patient privacy.

We receive clinical information from specialist medical practitioners who provide diagnostic reports, treatment recommendations, and other relevant information. General practitioners provide medical histories, current treatment plans, and clinical summaries that inform our assessments.

We may receive information from or provide information to other healthcare practitioners involved in your care, including allied health professionals, specialist consultants, and other medical practitioners, ensuring that all communications are properly authorised and documented in your medical record.

YOUR RIGHTS ABOUT YOUR PERSONAL INFORMATION

You may exercise certain rights regarding your personal information which we process. In particular, you have the right to withdraw consent where you have previously given your consent to the processing of your personal information, object to the processing of your personal information if the processing is carried out on a legal basis other than consent, learn if your personal information is being processed by us, obtain disclosure regarding certain aspects of the processing and obtain a copy of the personal information undergoing processing, verify the accuracy of your personal information and ask for it to be updated or corrected, restrict the processing of your personal information under certain circumstances, and obtain the erasure of your personal information from us under certain circumstances.

Access to Your Information

You have the right to request access to the personal information we hold about you. We will provide you with access to your personal information within a reasonable period, generally 14 days of

receiving your request, unless there are exceptional circumstances that require additional time for processing. We provide access to information in a format that is readily understandable and, where possible, in the format you have requested.

We may refuse to give you access to personal information in certain circumstances permitted under the Privacy Act, including where:

- giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- giving access would have an unreasonable impact on the privacy of other individuals;
- the request is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings;
- giving access would reveal our intentions in relation to negotiations with you in such a way as to prejudice those negotiations;
- giving access would be unlawful;
- denying access is required or authorised by or under an Australian law or a court/tribunal order, or
- we have a reasonable belief that there is an ongoing or potential unlawful activity or serious misconduct that could be impacted detrimentally by granting access.

If we refuse to give you access, we will provide you with reasons for our refusal, unless doing so would be unreasonable in the circumstances. We will also take reasonable steps to give you access in a way that meets your needs without giving rise to the reasons of our refusal. Further, we will provide details of how you may make a complaint about our decision.

Anonymity / Pseudonymity

Where lawful and practicable, you may request anonymity or the use of a pseudonym. However, in most cases QCC is unable to provide services anonymously (including where Medicare claiming or private health claiming requires identification matching government-issued records).

Correction of Your Information

You have the right to request correction of personal information we hold about you if you believe it is inaccurate, out of date, incomplete, irrelevant, or misleading. Our team aims to update information within a reasonable timeframe of receiving your correction request, and we will confirm with you in writing once the corrections have been made.

If we refuse to correct your personal information, we will provide you with written reasons for our refusal and information about how you can make a complaint about our decision.

Deletion of Your Information

You can request deletion of your personal information by contacting us at michelle.prado@qldchildrensclinic.com.au. However, we are required to retain clinical records in accordance with our retention obligations. We retain clinical records and personal information for 20 years after a patient turns 18 years of age. When personal information is deleted, we archive your patient profile while maintaining the clinical record for the required retention period. There may be circumstances where we cannot comply with deletion requests, such as where retention is required by law or where the information is necessary for legal proceedings.

HOW LONG DO WE KEEP YOUR PERSONAL INFORMATION

Information Retention Periods

As a healthcare provider, we maintain personal information in accordance with healthcare record retention requirements and professional obligations under Australian healthcare regulations.

Standard Retention Period

We retain all clinical records and personal information for 20 years after a patient turns 18 years of age.

Records of consent for information sharing, communication with healthcare providers, and other privacy-related decisions are maintained as part of the clinical record and are subject to the same retention periods. We are however committed to regularly reviewing and updating our information retention periods to ensure compliance with legal requirements and best practices in information protection.

Subject to our obligations under Australian law and our obligations stated above, personal information shall be processed and stored for as long as required by the purpose they have been collected for. We ensure that personal information is minimised to what is necessary during the retention period and securely deleted or anonymised when no longer needed. Personal information collected for the purposes of our legitimate interests shall be retained as long as needed to fulfil such purposes.

We will retain personal information for a longer period if we are required to do so by law or by an order from a legal authority. Exceptions to our standard retention periods may apply in cases of ongoing legal disputes, investigations, or other legitimate business needs that require extended retention. In such cases, we will retain the relevant information only for as long as necessary to fulfil these specific purposes.

Once the retention period expires, personal information is securely deleted through our information management systems. After the retention period expires, the information is securely destroyed or de-identified (where lawful and practicable).

SECURITY OF YOUR PERSONAL INFORMATION

We are committed to ensuring that the personal information we collect is secure. We take reasonable steps to protect your personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. We use a number of physical, administrative, personnel and technical measures to protect your personal information. These measures include:

Access Controls

Access to client records is limited to authorised personnel who require the information to perform their duties. Our practice management software, Genie, Heidi, and PracticeHub, and our internal systems on Microsoft Office are configured to restrict access based on roles. All access is logged and monitored to ensure accountability and prevent unauthorised access to personal information.

Our IT infrastructure, including email systems and cybersecurity monitoring, is managed by our Health IT provider under contractual confidentiality obligations.

Physical Security

We maintain physical security measures to protect our premises and data storage facilities. Our clinic has controlled access to the premises. Personal information is stored in both paper files and secure electronic databases. Our server infrastructure is cloud-based and managed through secure data centres that comply with industry standards for physical security. All paper-based records containing personal information are stored in secure locations with restricted access, and when no longer required, are securely destroyed or de-identified.

Staff Training

Our staff receive training on privacy and confidentiality obligations to ensure they understand their responsibilities in protecting your personal information. All staff are bound by confidentiality agreements and receive training on privacy obligations during their induction, which includes a review of our privacy policy. This ongoing training ensures that all personnel remain current with privacy legislation, best practices, and our internal procedures for handling sensitive health information. Staff are also trained to recognise and respond to potential privacy breaches.

However, we cannot be held liable for events outside our control, including security breaches of third-party systems, internet infrastructure failures, or other circumstances beyond our reasonable control. We will take reasonable steps to maintain the integrity and security of any personal

information we have stored, including taking reasonable steps to prevent interference and loss, misuse, unauthorised access, modification or disclosure of such personal information.

Internet Security

Note that no information transmitted over the Internet can be guaranteed to be completely secure. While we will endeavour to protect your personal information as best as possible, we cannot guarantee the security of any information that you transmit to us or receive from us. The transmission and exchange of information is carried out at your own risk.

It is important that you protect your privacy by ensuring that no one obtains your personal information, and you must contact us directly if your details change. Should your information be erroneously provided to us or no longer remain valid within the constraints of this Privacy Policy we will securely destroy or de-identify it as soon as practicable, as long as it is lawful to do so.

We have obligations to notify you if you are affected by a data breach. We will take all reasonable precautions to take remedial action to prevent such an event. However, as we cannot guarantee that remedial action will be sufficient to prevent all instances of a breach, we will take steps to notify you of an eligible data breach as soon as practicable, and provide recommendations as to what steps you should take to mitigate any serious issues.

DISCLOSURE OF PERSONAL INFORMATION OUTSIDE OF AUSTRALIA

We do not currently disclose personal information outside Australia. If overseas disclosure is required (for example, due to third-party technical support), we will take reasonable steps to ensure that the recipient complies with the Australian Privacy Principles or equivalent data protection laws.

AUTOMATED DECISION MAKING AND TECHNOLOGY-ASSISTED SERVICES

We inform you of the following automated systems that may be utilised in your care:

Communication and Reminder Systems

We utilise automated systems for sending appointment reminders and administrative communications via SMS and email. These systems are designed to support your healthcare journey and ensure you receive timely information about your care. You may opt out of non-essential automated communications while continuing to receive clinically important notifications.

No Automated Clinical Decision Making

We do not utilise automated systems for clinical decision making, diagnosis, or treatment recommendations. All clinical decisions, treatment plans, and healthcare recommendations are made by qualified allied health practitioners using professional clinical judgement and evidence-based medicine principles. We may offer telehealth consultations using secure, encrypted video platforms such as Zoom, and are exploring other compliant alternatives. Our current telehealth arrangements are configured so that information is not stored in the telehealth provider's systems, and we use secure Wi-Fi and network controls to protect information.

We can explain how automated reminder systems work and how to opt out of non-essential communications. We will provide additional information about our automated systems upon request and ensure that you maintain control over automated communications and processes that affect your healthcare experience.

WEBSITE AND DIGITAL PLATFORM PRIVACY

Our Website, currently under development, will include an enquiry form that collects personal information for the purpose of responding to enquiries. This information is used solely for responding to enquiries and is subject to the same security and privacy protections as all other personal information collected by our practice.

Our website may use cookies to improve user experience.

We utilise secure digital communication for appointment confirmations, cancellations, and reminders via SMS and email. These communications are generated through our practice management system and are subject to our standard privacy protections and security measures.

COMPLAINT PROCEDURES

If you have concerns about how we handle your personal information, you may lodge a complaint with us by contacting our Privacy Officer. We will investigate all complaints promptly and provide a formal response within a reasonable timeframe considering the circumstances, typically within 30 days of receiving your complaint.

Our complaint handling process includes acknowledgment of your complaint within 7 days, investigation of the matter by appropriate personnel, consultation with relevant staff and service providers where necessary, and provision of a written response outlining our findings and any corrective actions taken within a reasonable time.

If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner (OAIC) at enquiries@oaic.gov.au or 1300 363 992. You may also have rights to seek review through other regulatory bodies or legal proceedings as appropriate to your circumstances.

CONTACT INFORMATION

Enquiries, Requests & Complaints

Privacy Officer and Contact Information

Privacy Officer: Michelle Prado

Email: michelle.prado@qldchildrensclinic.com.au

Practice Manager: Cora Armstrong

Email: admin@qldchildrensclinic.com.au

Practice Name: Queensland Children's Clinic Pty Ltd

ABN: 12 819 485 767

ACN: 646 526 061

For all privacy-related enquiries, access requests, correction requests, complaints, or concerns about how we handle your personal information, please contact our Privacy Officer using the details above. We are committed to responding to all privacy-related communications promptly and professionally.

If you think your personal information, held by us, may have been compromised in any way or you have any other Privacy related complaints or issues, you should also raise the matter with the Privacy Officer.

If we do not resolve your enquiry, concern or complaint to your satisfaction or you require further information in relation to any privacy matters, please contact the Privacy Commissioner Australia, whose contact details are below.

Office of the Australian Information Commissioner

Telephone: 1300 363 992

Email: enquiries@oaic.gov.au

Office Address: Level 3, 175 Pitt Street, Sydney NSW 2000

Postal Address: GPO Box 5218, Sydney NSW 2001

Website: www.oaic.gov.au

DATE OF CURRENT VERSION: February 2026