Privacy Policy – RACF Visiting General Practitioner Services

Queensland Healthcare Pty Ltd

Document Owner	Dr Ash Kriplani (Principal GP / Director)
Version	1.0
Effective Date	[01/02/2026]
Review Date	[01/02/2029]
Next Scheduled Review	In Three Years (or earlier if required)
Applies To	All patients/residents seen by Queensland Healthcare Pty Ltd and any contracted staff supporting care delivery

1. Introduction

This Privacy Policy explains how Queensland Healthcare Pty Ltd (we, us, our) collects, uses, holds and discloses personal information, including sensitive information such as health information, when providing general practice medical services primarily to residents of Residential Aged Care Facilities (RACFs) and related stakeholders.

Queensland Healthcare Pty Ltd is a health service provider and is committed to protecting privacy in accordance with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth), and the relevant requirements of the RACGP Standards for General Practices (5th edition) where applicable.

2. How to contact us (privacy enquiries and complaints)

If you have a privacy enquiry, request, or complaint, please contact:

- Dr Ash Kriplani – Privacy Officer / Principal GP
- Phone: 07 3075 9991
- Mobile: 0406 903 467
- Email: enquiries@qldhealthcare.com.au
- Postal address: [Insert postal address]

3. Why and when your consent is necessary

When you receive medical services from us, you provide consent for us (and authorised members of our care team) to collect, use and disclose your personal information for the primary purpose of providing medical care and coordinating that care in the aged care setting.

Where information is needed for a secondary purpose that is not directly related to your care (and is not otherwise permitted by law), we will seek your additional consent.

Many RACF residents have impaired capacity or may have substitute decision-makers. Where you are unable to provide consent, we will work with your legally authorised representative (for example, Enduring Power of Attorney / Guardian) and follow relevant legal and ethical requirements.

4. Why we collect, use, hold and share your information

We collect and use your information to:

- Provide safe, high-quality medical care and clinical decision-making
- Coordinate care between your GP, RACF staff, contracted nurses, hospitals, specialists and allied health providers
- Prescribe medicines and arrange pathology, imaging and other investigations
- Support referrals, care planning and advance care planning (including goals of care and substitute decision-making)
- Claim Medicare rebates and meet billing/accounting requirements
- Meet legal and regulatory obligations (including mandatory reporting and notifiable conditions)
- Support accreditation, quality assurance, clinical audit, and service improvements

5. What personal information we collect

The information we collect may include (as relevant):

- Identification and contact details (name, date of birth, address, phone/email, next of kin)
- Medicare number, healthcare identifiers (IHI) and concession card details
- Medical history, diagnoses, allergies, immunisations, medications and adverse reactions
- Clinical notes, examination findings, care plans, referrals and correspondence
- RACF clinical information relevant to your care (including nursing notes, observation charts and medication charts)
- Hospital discharge summaries, specialist letters and diagnostic results
- Advance care planning documents (e.g., advance health directive, substitute decision-maker details, resuscitation plans)
- Information about service delivery or billing (appointment details, item numbers and accounts)

6. Dealing with us anonymously

Where practical and lawful, you may interact with us anonymously or using a pseudonym. However, because we provide medical services in RACFs (including Medicare claiming, prescribing and clinical risk management), it is usually not practical to provide full care without confirming your identity.

7. How we collect your personal information

We collect your information in a number of ways, including:

- Directly from you or your authorised representative
- From RACF clinical staff involved in your care

- From family members or substitute decision-makers (where appropriate)
- From other health service providers (e.g., hospitals, specialists, allied health, pathology and imaging providers)
- From government services (e.g., Medicare) and clinical information systems used for prescribing and claiming
- From My Health Record (where available and appropriate, and subject to your My Health Record settings)
- Through secure phone, electronic communication or digital forms where required

8. Digital health systems and communications

We use clinical information systems to document consultations, manage prescriptions, generate referrals, and support care coordination. This may include secure messaging, electronic prescribing and (where applicable) access to and uploading to My Health Record.

If we communicate with you, your representative, or RACF staff via email or other electronic means, we take reasonable steps to ensure communications are secure. However, electronic communications can carry risks. If you prefer not to receive information electronically, please let us know.

9. Sharing (disclosing) your information

Your personal information may be shared with other organisations or individuals involved in your care, including:

- RACF clinical staff involved in your day-to-day care
- Contracted nurses engaged to support service delivery
- Hospitals, specialists and allied health professionals (with your consent where required)
- Pathology and medical imaging providers
- Community or hospital pharmacies (including e-prescribing and medication supply arrangements)
- Ambulance services and emergency departments where necessary for urgent care
- Third-party service providers who support our operations (e.g., IT support, secure clinical software providers, billing or administrative support) who are bound by confidentiality and only access information necessary to perform their functions

At times, Queensland Healthcare Pty Ltd may be supported by GP Aged Care Network Pty Ltd to provide administration, stakeholder and nursing supports. Where this occurs, access to personal information is limited to what is necessary to support care delivery and practice operations, and relevant confidentiality and security requirements apply.

We may also disclose information where required or authorised by law, including for notifiable conditions, mandatory reporting obligations, subpoenas/court orders, or to prevent or lessen a serious threat to life, health or public safety.

10. Disclosure outside Australia

We do not generally disclose your personal information outside Australia. If an overseas disclosure is required (for example, because a service provider stores data overseas), we will take reasonable steps to ensure the recipient handles your information in a way that is consistent with the Australian Privacy Principles, and we will obtain your consent where required.

11. Use of de-identified information for quality improvement

We may use de-identified information (information that cannot reasonably identify you) for quality improvement, clinical audit, accreditation activities and service planning. If you do not wish your de-identified information to be used in this way, please notify us and we will take reasonable steps to exclude it where practicable.

12. Data storage, security and retention

We store personal information in secure electronic medical record systems and, where applicable, secure cloud-based platforms used for clinical and administrative purposes. Access is restricted to authorised personnel.

We take reasonable steps to protect information from misuse, interference and loss, and from unauthorised access, modification or disclosure, including:

- Role-based access controls and user authentication
- Secure devices and encryption where appropriate
- Confidentiality obligations for staff and contractors
- Secure disposal of information when it is no longer required
- Policies for managing privacy and information security incidents

We retain health records for the periods required by law and in accordance with professional and accreditation requirements. When information is no longer required, it is securely destroyed or de-identified.

13. Accessing and correcting your information

You have the right to request access to the personal information we hold about you and to request correction if you believe it is inaccurate, incomplete or out of date.

To request access or correction:

- Contact us using the details in Section 2.
- We may ask you to submit the request in writing and to verify your identity or authority to act.
- We aim to respond within 30 days. A reasonable fee may apply for large or complex requests (for example, copying).

If we refuse access or correction, we will explain the reason (where permitted) and how you may make a complaint.

14. AI-assisted clinical documentation (if used)

Some clinicians may use approved clinical documentation tools (including AI-assisted drafting tools) to support the efficiency and accuracy of consultation notes. These tools do not replace the clinician's judgement. Clinicians must review and approve all notes before they are added to the medical record.

Where an AI-assisted tool is used, we will seek patient consent where appropriate, and we will apply safeguards to protect privacy and confidentiality.

15. Making a privacy complaint

If you believe your privacy has been breached, please contact us in writing or by phone using the details in Section 2. We will acknowledge your complaint within 7 days and aim to respond within 30 days.

If you are not satisfied with our response, you may contact:

- Office of the Australian Information Commissioner (OAIC) – Phone: 1300 363 992 – Website: www.oaic.gov.au
- Office of the Health Ombudsman (Queensland) – Phone: 133 OHO (133 646) – Website: www.oho.qld.gov.au

16. Website and digital communications

We may collect basic information through our website or digital forms (for example, name and contact details for enquiries). We may also collect usage data through cookies or analytics tools to improve our services. We do not collect or store identifiable health information through a public website unless this is done through a secure, authorised system.

17. Optimising privacy during consultations

We aim to conduct consultations in a way that protects each resident's dignity and confidentiality. Our visiting GPs, Nurse Practitioners (NPs) and other clinicians (together, Providers) take reasonable steps to optimise privacy during consultations, noting that the RACF environment may sometimes limit complete privacy.

During consultations, Providers will, where clinically appropriate:

- ask the resident (and/or their substitute decision-maker) who they would like to be present and obtain consent before discussing sensitive information with RACF staff, family members, carers, interpreters, or others;
- use a private space (for example, the resident's room with the door/curtain closed or a designated consultation room) where available, and speak discreetly to reduce the chance of being overheard;
- limit discussions of personal and health information in hallways or communal areas, and avoid being overheard by other residents, visitors, or staff who are not involved in the resident's care;
- position screens and paperwork to prevent unauthorised viewing, and avoid leaving documentation unattended;
- where phone or video consultations are used, take reasonable steps to maintain privacy (for example, confirming identity, using a private area, and ensuring conversations cannot be overheard); and
- document and manage any situations where full privacy is not possible (for example, where staff need to be present for resident safety or clinical care), and limit disclosures to what is necessary.

We also work with the RACF to support privacy by [insert your process – for example, requesting an

appropriate private space, scheduling consultations to reduce interruptions, and limiting the number of people present].

18. Policy review statement

This policy is reviewed at least every three years and whenever there are material changes to how we handle personal information, or when relevant regulatory requirements change. The current version is available on request.