PATIENT INFORMATION AND PRACTICE POLICY

IFH & BFH

Privacy Policy

Innisfail Family Health and Babinda Family Health

VERSION	CURRENT AS OF	NEXT REVIEW
2.5	12 October 2026	12 October 2027

INNISFAIL FAMILY HEALTH (IFH)
65-67 Edith Street, Innisfail QLD 4860
Phone: (07) 4061 2985
Fax: (07) 4061 8836
Email: admin@innisfailfamilyhealth.com.au
innisfailfamilyhealth.com.au

BABINDA FAMILY HEALTH (BFH)
Shop 2A, 93-95 Munro Street, Babinda QLD 4861
Phone: (07) 4234 4888
Fax: (07) 4234 4801
Email: adminbfh@innisfailfamilyhealth.com.au
babindafamilyhealth.com.au

Privacy in brief

- We collect personal and health information reasonably needed to provide safe care and run the practice.
- We protect your information and limit access to authorised people who need it for their work.
- We use and share information for healthcare, directly related purposes you would reasonably expect, and where consent or law permits or requires it.
- You may ask to access or correct your information, change communication preferences, or make a privacy complaint.
- Lyrebird may help prepare consultation notes only with informed consent at each consultation. You may decline or withdraw consent without affecting your care, and your doctor checks and approves the note.

This policy is available without charge at either practice, on our websites, and in an accessible format on request. Specific services or technologies may also have a separate collection notice.

1. About this policy

We are Innisfail Family Health (IFH) and Babinda Family Health (BFH). This policy explains how we handle your personal information, including health information, and how you can access or correct it or raise a concern. It applies to patients, representatives, carers, visitors and people using our websites or contacting either practice.

We follow the Privacy Act 1988 and Australian Privacy Principles, together with applicable health, My Health Record and other laws. Our staff, practitioners, contractors, students and service providers must protect the information they handle for us. This policy is available free at both practices and on our websites, with accessible formats available on request.

2. Information we collect and hold

We collect information reasonably needed for healthcare and related practice activities. Depending on your dealings with us, this includes:

- Identity and contact details, date of birth, relevant sex or gender information, communication and language needs, emergency contacts, and information needed to verify a representative's authority.
- Medical and family history, symptoms, diagnoses, medicines, allergies, results, referrals, clinical notes, care plans, images and other information relevant to your care, including sensitive health information.
- Relevant cultural and demographic information, including Aboriginal and Torres Strait Islander status; Medicare, DVA and healthcare identifiers; appointments, accounts, payments, consent and communication preferences.
- Information from online forms, bookings, secure messages and telehealth; clinical photographs or audio and video where consented to or otherwise lawful; and technical information from our digital services where collected.
- Complaints, feedback, incidents, security logs and, where cameras are installed, footage from designated non-clinical areas.

Patient records may include information about family members or other people. We protect their information too and may need to limit access or disclosure to protect confidentiality or comply with the law.

3. How we collect information

We usually collect information directly from you through forms, consultations, calls, correspondence and digital services. Where direct collection is not reasonable or practicable, we may collect from an authorised representative, another treating provider, My Health Record, Medicare, DVA, insurers, an approved service provider or a lawful public authority.

If we receive information we could not lawfully have collected, we securely destroy or de-identify it where lawful and reasonable. If you do not provide information we need, we may be unable to provide safe care, contact you, issue prescriptions or referrals, or process a claim.

4. Why we use information and when we share it

Our main purpose is to provide, coordinate and document your healthcare. We also use information for directly related purposes you would reasonably expect, or where consent or law permits or requires it. These include results, recalls and reminders; referrals; billing and claims; practice administration; quality improvement, clinical audit and accreditation; staff education; complaints and incidents; information security and recovery; and legal, public-health and professional obligations.

We share only information reasonably necessary for the purpose. Recipients may include treating healthcare providers, Medicare, DVA, My Health Record and identifier services, authorised insurers, a person you authorise, or a representative whose legal authority we have verified. Approved service providers may handle information to support our clinical, booking, communications, IT, hosting, administration and professional services.

The law may permit or require disclosure without consent, for example for a court order, mandatory public-health or child-protection report, a serious threat to health or safety, or another legally permitted situation. Each disclosure must have a lawful basis.

We use de-identified or grouped information for quality improvement and education where practicable. Identifiable research requires consent or another lawful authority and any required ethics and governance approval. Access by authorised auditors or advisers is limited and subject to confidentiality obligations.

We do not sell patient information. We use health information for direct marketing only with consent, which you may withdraw at any time. Healthcare recalls, reminders and necessary care communications are not marketing.

5. Your choices and consent

Consent must be voluntary, informed, current and given by someone with capacity or lawful authority. Depending on the circumstances, it may be express or implied. We seek express consent when required, including for specified recording and digital functions or a practice-introduced third party in a consultation. You may withdraw consent for future handling; this does not undo earlier lawful handling.

You may use a pseudonym or remain anonymous where lawful and practicable. Identification is usually needed for safe ongoing care and may be required for prescriptions, referrals, claims and digital health services. We will explain any limitation.

We consider a child or young person's capacity and confidentiality rights. We verify a parent, guardian or other representative's authority. A family member, next of kin or carer is not automatically entitled to information. We obtain appropriate consent for an interpreter, chaperone, student or observer. Refusing a student or observer does not disadvantage your care.

6. Digital health and communications

Messages and online services

We check identity before discussing or releasing personal information and use secure clinical messaging where appropriate. Email and SMS can be misdirected, intercepted or seen on shared devices. We minimise sensitive content, check contact details and consider urgency. Tell us your preferred contact method and restrictions; clinically important matters may require another reasonable method.

Website forms and booking information are used to respond or provide the requested service. External platforms may have their own privacy policies. Please contact the practice directly rather than using social media for private health information or clinical advice.

Telehealth and recordings

We use approved telehealth systems and confirm identity and who is present. We do not make, duplicate or store consultation audio or video without prior informed express consent from the patient and anyone else recorded. We explain the purpose, service provider, handling, access, storage and withdrawal arrangements and record consent or withdrawal in the patient record. Apart from separately consented scribe use below, we do not routinely record telehealth consultations.

My Health Record and clinical documents

Where our systems participate, authorised staff use My Health Record only for permitted healthcare purposes and respect patient instructions and access controls. We maintain a separate security and access policy, train authorised users and remove access when no longer needed. Clinical systems may fill documents from your record; the responsible clinician checks accuracy and relevance before release.

The Lyrebird clinical scribe

Your doctor may ask to use Lyrebird Health, an approved external AI-assisted note-taking service. At each consultation, before capture or processing starts, we obtain and document informed consent from you and anyone accompanying you whose voice may be captured. We explain how audio and text will be processed, duplicated or temporarily stored. You may decline or withdraw consent without affecting your care.

Lyrebird captures consultation audio and converts it to text in real time to prepare a preliminary clinical note. Its published information states that Australian data is processed and stored in Australia, audio is discarded after transcription, and customer data is not used to train or fine-tune AI models. These notes are encrypted and retained for the period configured by the practice before transfer or deletion. We review the settings and provider terms periodically.

The doctor checks, edits and approves the note before it enters your record and remains responsible for clinical decisions. We may avoid scribe use where capacity, safeguarding, sensitive information or the consultation setting creates a privacy concern. Patient information must not be entered into public or unapproved generative AI services. New tools and material changes require privacy and security assessment before use.

Software that makes or assists significant decisions

We will assess whether any software uses personal information to make, or substantially and directly contribute to, decisions that could significantly affect a person's rights or interests. Human review alone does not exclude a use from these rules. Where a use is in scope, we will describe the information used and the kinds of decisions made entirely by software or assisted by it before the new transparency requirements begin on 10 December 2026. Our Quality Improvement Leader is responsible for this assessment.

7. Overseas handling

We seek Australian-hosted services for clinical information where reasonably available. We do not intentionally send health information overseas as part of routine clinical care. Some approved providers may, however, use overseas support, subcontractors or infrastructure. We assess these arrangements under privacy law before use.

Where overseas disclosure is likely, our policy will identify the countries where practicable, with a specific collection notice where relevant and consent where required. If you request a transfer to an overseas treating provider, we confirm your authority, explain material risks where appropriate and use a reasonably secure method.

8. Security and record retention

We take reasonable steps to prevent misuse, loss, interference and unauthorised access, change or disclosure. These include access limited by role, individual accounts, authentication, audit logs, device and network protection, secure messaging, physical security, backups, confidentiality agreements, training and controls for service providers.

Our practice minimum is seven years from the last clinical entry for adult health records. Records created while a patient was under 18 are retained until at least their 25th birthday, or when they would have reached that age. We keep records longer where clinically appropriate or required for a legal hold, claim, complaint, investigation, contract, insurance or other lawful need. These are practice minimums, not a statement that every record may be destroyed at those dates.

When information is no longer needed and no lawful retention reason remains, we securely destroy or de-identify it. Confidentiality continues after death.

9. Privacy incidents

We promptly contain and investigate suspected breaches, assess harm and take corrective action. Where an eligible data breach is suspected under the Privacy Act, we take reasonable steps to complete the assessment within 30 calendar days. If notification is required, we notify the OAIC and affected people as soon as practicable. My Health Record breaches follow a separate notification process involving the System Operator and OAIC. Contact either practice promptly if you suspect information has been lost, misdirected or accessed improperly.

10. Access correction and transfer

Contact our privacy contact through either practice to request access or correction. A written request helps us identify the records and format you want, but we assist with other reasonable forms of request. No reason is needed to request access. We check identity and any representative's authority and generally respond within 30 calendar days.

There is no fee to make an access request. A reasonable, non-excessive charge may apply to providing access; we explain it beforehand. We provide access in your requested manner where reasonable and practicable, or consider alternatives. If access is refused, we give written reasons and complaint options where required.

You may ask us to correct information that is inaccurate, out of date, incomplete, irrelevant or misleading. Correction requests are free. We preserve the record's history through corrections or addenda. If we refuse, we explain why and provide complaint options where required. You may ask for a statement of the requested correction to be associated with the record and for relevant previous recipients to be notified where reasonable and practicable.

With valid authority, we securely transfer a copy or appropriate summary to another healthcare provider in a timely manner. We normally retain the original under our retention obligations.

11. Privacy questions and complaints

Please ask for the Practice Manager, our privacy contact, through either practice using the contact details on the first page. Tell us your concern, the relevant information and dates, how to contact you and the outcome you seek. We acknowledge and investigate complaints fairly, keep you informed and aim to give an outcome within 30 calendar days. If more time is needed, we explain why and the next step.

If you are dissatisfied, you may contact:

Organisation	When to contact	Contact
Office of the Australian Information Commissioner (OAIC)	Privacy complaints and Australian Privacy Principles matters	1300 363 992 oaic.gov.au
Office of the Health Ombudsman (Queensland)	Complaints about a Queensland health service or provider	133 OHO (133 646) oho.qld.gov.au

12. Availability and review

Ask reception for a free paper copy, accessible format or help understanding this policy, including interpreter assistance. We review it at least annually and after material changes or significant privacy incidents. Applicable law prevails if there is any inconsistency.