



Lakeside Medical Practice Warilla

Email Policy

This policy outlines the appropriate use, management, and security of email communication at Lakeside Medical Practice to ensure safe, respectful, and confidential interactions with patients, staff, and third parties. It supports compliance with RACGP Standards, privacy legislation, and best practice guidelines for secure information exchange. This policy applies to all staff, contractors, and healthcare providers using email for clinical or administrative purposes at Lakeside Medical Practice.

General Principles

- Email is not the preferred method for urgent or emergency communications.
- All email communications must comply with the Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs).
- Email correspondence should maintain a professional tone and adhere to our standards of respectful and culturally appropriate communication.

Patient Email Communication

Patient Consent

- Email communication with patients will only occur if the patient has provided documented informed consent.
- Patients must be informed about the risks of unencrypted email, including the possibility of interception.

Information Sent by Email

- Emails may be used to send:
 - Appointment reminders (if opted-in)
 - Health education materials
 - Administrative forms or documents
 - Non-sensitive follow-up information
- **Clinical information, test results, or referrals** will only be sent via email if:
 - Consent is documented
 - The email address is verified
 - The message is de-identified or password-protected where appropriate

Patient Responsibility

- Patients are advised to check their email regularly.
- They are encouraged to notify the practice of any changes to their email address.

Practice Responsibility and Procedures

Checking and Responding to Emails

- Emails to the practice are checked at regular intervals throughout the business day by designated administrative staff.

- All incoming patient emails are acknowledged within one business day, with clinical matters triaged or referred to the appropriate provider.

Outgoing Emails

- All outgoing emails must:
 - Include the practice's email disclaimer
 - Be sent using the official practice email account
 - Be recorded in the patient's medical file, where appropriate

Security Measures

- Practice computers and email systems are protected by anti-virus software, firewalls, and secure access protocols.
- Staff must not use personal email accounts for practice-related communication.
- Emails containing sensitive or confidential information should be encrypted or password-protected where feasible.