



Email Policy

Purpose

This policy outlines how our practice manages privacy and security in email communications. It has been developed in alignment with the RACGP 5th Edition Standards and AHPRA guidelines to ensure best practices in handling sensitive health information.

Background

Email has become a common method for patients, healthcare providers, and third parties to request or exchange health information due to its convenience. However, the Australian Privacy Principles (APPs), published by the Office of the Australian Information Commissioner (OAIC), recognise that health information is among the most sensitive types of personal data. Consequently, appropriate safeguards must be in place when using email to protect patient privacy and maintain confidentiality.

Email Configuration and Communication Practices

Secure Clinical Messaging:

Where possible, all clinical communications between healthcare providers are conducted through secure clinical messaging systems such as HealthLink, integrated within the practice's clinical software. This ensures communications are automatically recorded in the patient's medical file.

Email Communications with Patients:

Email communication with patients has increased, particularly during the COVID-19 pandemic. This includes the transmission of referrals, prescriptions, and other documents.

To manage the associated risks, we have implemented the following safeguards:

1. **Computer Security:** All practice computers have up-to-date antivirus and cybersecurity measures in place.

2. 2. Patient Identification: We verify patients using at least three identifiers (e.g. name, date of birth, address) before sending personal information.
3. 3. Risk Notification: Patients are informed that emails are not encrypted and therefore may carry a privacy risk. They may choose to collect hard copies in person if preferred.
4. 4. Misaddressed Emails: A warning is included in all outgoing emails in case an email is sent to the wrong recipient.
5. 5. Encrypted Documents: Where feasible, patient information (e.g. test results, medical certificates, referral letters) is sent as encrypted attachments. Patients are provided with the required passcode to access these documents securely.

Email Disclaimer

All practice-affiliated emails include the following disclaimer:

PRIVACY & CONFIDENTIALITY NOTICE

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient, you have received this email in error. Any use, dissemination, forwarding, printing, copying, or handling of this email in any way is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the sender.

It is the responsibility of the recipient to scan this email and any attachments for viruses and defects before use. The practice does not warrant that this communication is virus-free or error-free. Any views expressed in this email are those of the sender, unless expressly stated otherwise.

Policy Review Statement

This policy is reviewed annually, or earlier if there are changes to legislation, technology, or clinical procedures that impact email communication practices.