



PRINTED COPIES ARE NOT CONTROLLED

:

## ***Patient Electronic Contact Policy and Procedure***

# **Policy**

Email may be used by a practice to transmit information outside the practice.

Ideally communication should be via secure messaging or encryption but this is generally not possible when emailing patients.

The practice has an obligation to take reasonable steps to protect the privacy and security of information it holds including when it is transmitted or disclosed outside the organisation.

The practice follows the RACGP recommendations to reduce the risk of interception of data and sending emails to incorrect addresses, including:

- use of passwords for sensitive information
- verification of the patient's email address
- obtaining patient consent
- use of secure messaging facilities between practices where available

The practice website is enabled to allow patients to email the practice, as standard response if provided to patients.

In addition, a member of the practice team is responsible for monitoring and managing responses to emails received via the practice website.

# **Procedure**

### **Request for information to be sent via email**

If a patient requests information to be sent by email, the practice:

1. Explains to the patient that email is not a secure form of communication
2. Seeks the patient's consent in writing to use email and asks the patient to provide the email address they would like the practice to use (in the same way the practice asks for a contact phone number)
3. The patient needs to acknowledge in the email that they understand the email returned will not be encrypted and that they accept to receive it via email anyhow
4. Notes that sensitive information will be sent by password protected PDF
5. Phones the patient to provide the password to open the PDF.

The practice should document the patient consent and maintain a record of information sent via email to the patient in accordance with the email policy.

### **Patients emailing the practice via the practice website**

The practice advises patients via the practice website of the risks of sending clinical information via unencrypted email. The message addresses the issue of patient choice, including the ability of patients to choose what medium of communication to be used to send their own personal information to them. A suggested auto reply would be along the lines of:

"This email address is not regularly monitored and is not our preferred means of communication. There is a risk that important clinical information sent to this address may be missed or not picked up, particularly time critical information. In addition we urge all patients to carefully consider the issue of security before sending medical information via unencrypted email. The alternative methods

for communicating clinical information are below although please do not use normal post for forwarding time critical information. We encourage patients to phone the practice or make an appointment to discuss clinical issues."

Our Practice Manager is responsible for replying and addressing issues received via email correspondence.

**Related page:**

[Request for personal health information](#)

**Helpful resources:**

[Using email in general practice – privacy and security matrix](#) (RACGP)