

Email Policy

In our practice we do use emails as a method of communication as it is becoming an increasingly more popular request from patients.

Emails are accessible to staff on password protected computers which are only available to authorised staff.

General practices must consider their obligations under the Privacy Act before they use or disclose any health information.

The Privacy Act does not prescribe how a healthcare organisation should communicate health information. Any method of communication may be used as long as the organisation takes reasonable steps to protect the information transmitted and the privacy of the patient.

A failure to take reasonable steps to protect health information may constitute a breach of the Australian Privacy Principles and may result in action taken against the organisation by the Australian Privacy Commissioner. What amounts to reasonable steps will depend on the nature of the information and the potential harm that could be caused by unauthorised access to it.

The RACGP has developed a matrix is to assist practices in determining the level of security required in order to use email in general practice for communication.

We have signage in our waiting room that requests patients update any details if they have changed and emails are requested on the new patient form. If a patient does request to have something emailed to them, we do ask them to reconfirm their email address.

In our practice we inform patients of possible risks to their privacy if standard unencrypted email is used.

Before any information is sent to the patient via email the patient must sign an email consent form and the employee whom has obtained the consent must document in the patients record when scanning in the consent that they "discussed the privacy risks of the use of encrypted or unencrypted email, patient is aware of same and requests the use of encrypted or unencrypted email for communication"

Practice staff should warn patients of the following possible risks:

Other people possibly gain access to the patients email and can access information communicated from the medical centre.

The information can be hacked due to being via electronic transmission



Power Medical Centre

There is a risk to others having access to private and confidential records due to electronic transmission.

In our practice we do use password protection for any documentation that will be sent to the patient.

This includes encryption in both word and adobe PDF documents.

Authorised staff are aware of how to encrypt the documents and keep a list of passwords available.

The consent form required by patients to sign is available to staff.