Email Policy

Practice Email Policy

Considerations: Patients, staff and collaborating treatment providers may expect or seek the use of email to manage their health care and health information. Although this is sometimes based on convenience and ease of use, it is important to recognise that such communications when unencrypted may result in access / interception by unauthorised parties and this would represent a breach of Australian Privacy Laws. Staff should communicate this to patients when relevant so that they understand the limitations of sending us information using this method. It is not our policy to send clinical information to patients via email so as to minimise the risks inherent to this practice including, but not limited to, privacy and security considerations.

We are able to communicate with medical consultants using health link via our Medical Director Software platform. This is encrypted to provide a high level of security.

It is not our policy to use email for management of patient information. Where a patient sends information to us via email, it is policy to advise the patient of the inherent risks of such a practice and recommend either delivery of the information via USB / CD / or indeed via permission based access to their online My Health Record where this information can be accessed, if available, with download to their clinical file in our Medical Director software, where relevant.

Other options for the safer transmittal of confidential medical information include facsimile and post. These are the preferred alternative methodologies for communication.

This policy is informed by the online publication “Using email in general practice – privacy and security matrix”.