

Pioneer Health Albany's Email Policy is in place to ensure reasonable steps are taken to ensure the communication of personal health information via email is safe and secure. It is, however, critical that GPs, staff and patients are aware of the associated risks with using email to send personal health information.

The Privacy Act (1988) does not prescribe how a healthcare organisation should communicate health information to patients or third parties. Any method of communication may be used as long as the organisation takes reasonable steps to protect information transmitted and the privacy of the patient. These reasonable steps are outlined in the below policy.

## Purpose

Our practice is increasingly receiving requests from patients and providers to send personal health information via email. Pioneer Health Albany is required to adhere to the Privacy Act 1988 (Privacy Act) and as such has protocols and precautions in place to ensure this information is sent as securely as possible, with informed consent obtained from the patient.

The practice also transmits traditional faxes via fax to email as a result of transitioning to VOIP services throughout the practice.

This policy applies to all requests for sending of personal health information to a patient and or third party service provider via email or fax to email. This policy applies to all employees of Pioneer Health Albany.

All email communication undertaken with patients require the following:

- Risks associated with sending personal health information are explained to the patient (i.e. Pioneer Health cannot guarantee privacy for emailed information)
- The patient accepts the risks and consent is obtained and recorded in the patient file

- Email address is verified by the practice and information is sent via "reply" to the original request;
- If the document contains sensitive information, or if the patient requests password protection, the document containing personal health information is converted to PDF and password protected prior to sending using Adobe Acrobat. The password for accessing the document is sent to the patient via SMS on mobile number verified by the practice.

With these controls in place the risk is considered LOW in accordance with the RACGP Privacy and Security Risk Matrix.

## Third party requests

In the event an allied health provider, specialist or other health care professional requests information to be sent via email, the procedure for sending password protected pdf files via email or including a PIN when sending direct from Best Practice, must also be followed.

Steps taken by the practice to ensure patients privacy and security is protected include:

- Setting up and saving contact email/fax addresses for third parties whom we correspond with
- Double checking fax number/email address prior to sending
- Ensuring clinical information requested is sent as an attachment to the email and never forms part of the body of the email
- Use of a privacy disclaimer on all emails/fax to email for unintended recipients
- Recording of all incoming and outgoing emails/fax to emails in the patient clinical record.

Whilst the practice supports the sending of information via email, or fax to email, to ensure time critical information is received in such a manner as to optimise patient outcomes it is

always the preference of the practice to utilise our secure messaging platform, Health Link, to send encrypted health information to third parties.

Other measures in place to ensure privacy considerations are met include;

- Ensuring clinical information requested is sent as an attachment to the email and never forms part of the body of the email;
- Reply all is never utilised when responding to an email that includes clinical information;
- Double checking email address prior to sending information;
- Where appropriate (highly sensitive information) seeking approval from the patient prior to emailing health information to a third party provider. This is to be balanced against the potential compromise to patient care and safety that might occur if significant information is not received in a timely manner.

## **Breach**

In the event of a privacy breach, Pioneer Health Albany's Data Breach Response Procedure is to be followed.