Avant factsheet:
Email communication with patients policy checklist

To satisfy your privacy obligations, your practice should develop a policy and procedures to manage communication by email.

Your policy and procedures manual should include:

- ☐ A statement as to when you and your team are willing to respond to email requests from patients (this will depend on the size of the practice and the ability to monitor emails and respond in a timely manner).
- ☐ What sorts of information will be sent by email and the level of protection required – encryption, secure messaging, password-protected attachments.
- ☐ If using passwords to protect a file outline the protocol on how that password is chosen and communicated to the patient.
- ☐ How you will confirm and document patient consent to communication by email.
- ☐ Steps staff need to take to avoid data breaches – checking email addresses, avoiding auto-complete text in addresses.

  Refer to our article: 7 steps to avoid a human data breach
- ☐ How you will ensure that electronic communications, including email and attachments, are retained, stored and destroyed in accordance with record-keeping requirements.

  Refer to our factsheet: storing retaining and disposing of medical records
- ☐ Which staff are approved to send or reply to patient emails.
- ☐ Criteria for when patient emails must be referred to a doctor or other clinician for action.
- ☐ How you will respond to requests if you are unwilling to send information by email – whether because of practice capacity or because of the particular circumstances.
- ☐ When you will require confirmation of receipt, for example, for time-sensitive information.
- ☐ How you will manage and communicate about your use of practice email addresses – including auto-replies and ongoing monitoring of website email.
- ☐ Your policy if a data breach occurs via email with reference to your data breach policy.

  See our information on data breaches
- ☐ Outline the exact wording for your practice privacy. disclaimer to be included at the end of each email.

Disclaimer example

This communication is confidential and intended only for the individual or entity to whom it is addressed. No part of the email should be copied, disclosed or redistributed without [PRACTICE NAME'S] authorisation. If you have received this in error, please notify the sender of its incorrect delivery by reply email or phone [PRACTICE PHONE NUMBER].

Note: This email is only viewed once a day by a non-clinical staff member. Please do not send clinical queries via email.

More about encryption

Email travels from your local computer to your server; to the patient's server; to the patient's local computer – so a four-step process. Email encryption can occur in two main areas, during transmission and/or during storage. Often encryption is happening without you being aware. Most email servers today such as Gmail and Outlook employ transport-level encryption. This means that the email is encrypted in transit from you to the server. It's not a total solution, as the contents of the email are potentially accessible on the server. End-to-end encryption is a lot safer, which means the email is encrypted throughout the entire trip.

If your medical practice has email encryption software, it will generally mean you have end-to-end encryption. When you send an email to a patient it is safe until it reaches the patient's inbox. Some encryption software will self-decrypt at this point or the patient may have to go through an extra step to access the encrypted email. If you are interested in installing encryption software, speak with your IT provider/specialist.

Any email the patient returns to you is likely to be unencrypted (unless they have encryption software). They need to be aware of this.

Additional resources

You can find additional resources including articles, podcasts and webinars in the **Avant Learning Centre** under technology or communication headings.

Avant Email communication with patient's: privacy and patient safety factsheet

Avant Recommendations when using SMS messaging factsheet

Avant Cyber Security – what you need to know

Office of the Australian Information Commissioner, Guide to Securing Personal Information

Royal Australian College of General Practitioners, Using email in general practice

MJN372 07/20 (DT-1459)