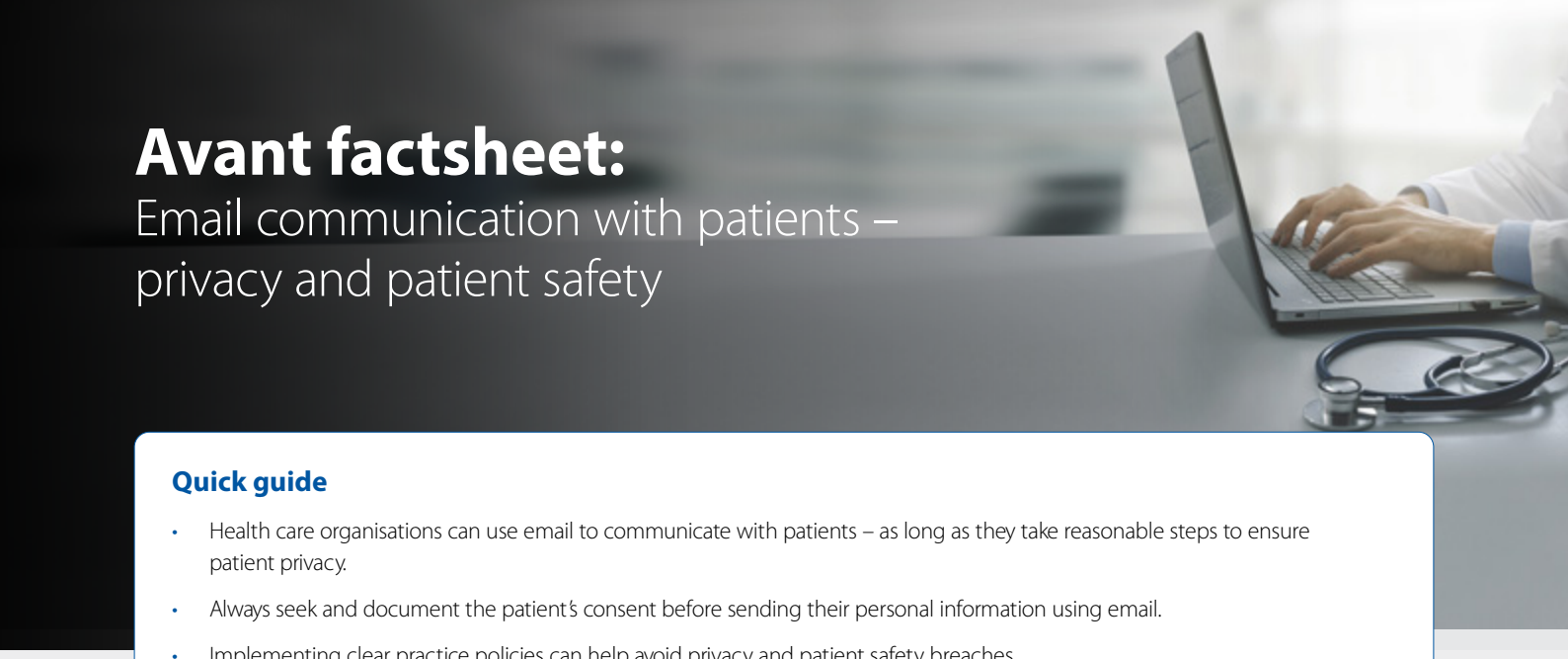
Avant factsheet:
Email communication with patients – privacy and patient safety



Quick guide

- Health care organisations can use email to communicate with patients – as long as they take reasonable steps to ensure patient privacy.
- Always seek and document the patient's consent before sending their personal information using email.
- Implementing clear practice policies can help avoid privacy and patient safety breaches.

Can you use email to communicate with patients?

Patients are increasingly expecting their doctors to communicate via email as it is often easier and more convenient for them. Consultations via telehealth rely increasingly on email to communicate with patients and other health professionals. However, you may worry about whether you can send information by email or you may think that you can only use encrypted email.

In fact, privacy legislation does not prescribe how you or any health care organisation should send health information to patients or third parties. The law states that any method of communication can be used so long as you take reasonable steps to protect the privacy of the patient and the security of their health information. So, yes, you can email your patients.

Satisfying your privacy obligations – reasonable steps

The Office of the Australian Information Commissioner ('OAIC' – which includes Australia's Privacy Commissioner) has outlined the steps it considers reasonable for organisations to take when communicating by email in its Guide to Securing Personal Information. In line with this guide, we recommend:

1. Email encryption is ideal but not essential

Using encryption is the safest way to send an email and you should use it wherever possible.

However, the OAIC does not insist that healthcare organisations use encryption as a minimum standard in all cases. Rather, you need to "develop procedures to manage the transmission of personal information via email", recognising that email is not necessarily a secure form of communication.

You do need to consider the type of information and whether it is appropriate to send by unsecured email, or whether you need to take additional steps to protect it by attaching the information as a PDF document with a password. How you provide the appropriate password to the patient is another consideration, but options could include a separate email, an SMS or something elected by the patient and stored in your system.

2. Have a clear policy

Just because it is easy to send an email does not mean it is appropriate. For this reason, you need to develop practice policies about the appropriate use of email to communicate with patients. All staff need to be clear about what they can and cannot send by email, and the steps they need to take if they are using email.

Even if your practice does not correspond by or encourage email, you may still receive email from patients, so it is important that your policies address how email will be managed.

3. Make sure you have patient consent

You may need to send information by email, for example as part of a telehealth consultation, or in response to a patient request. In this case, you should advise the patient about the risks associated with unencrypted email and confirm they still wish to have the information sent in that way.

Ideally, you would get patient consent in writing. If that is not practical, make sure you get the patient's verbal consent and document it in their clinical record.

However, when sending a patient information via email, if you have any concerns about their understanding and informed consent about the specific email, reconfirm details and consent with patient prior to sending.

4. Check the address before pressing send

The OAIC consistently reports that private information being sent to the wrong recipient accounts for around one in 10 data breaches.

Another emerging theme is errors involving auto-complete – where software programs default to recently or frequently used addresses.

Other sources of error could involve misheard or mistyped email addresses, or accidentally using 'reply all'.

Patients may have more than one email address. They may not want information sent to a work or shared email for example, so make sure you check which address they want you to use.

Useful tip to avoid incorrect email address

To avoid such errors, you could ask the patient to email you requesting the information and giving consent to reply using email. This serves both as a record of the patient's consent and confirmation of their preferred email address.

5. Password protect sensitive information

Your policy needs to address whether and how you will send particular types of information, for example results, prescriptions, or referrals.

Some clinical or sensitive information should ideally be sent in a password-protected file. You will need to make this determination. In this case, make sure you take care to avoid including sensitive information in the body of the email.

Your process also needs to include a protocol for providing the password (for example, phone the patient with the password).

6. Use a privacy disclaimer

The best course is to avoid sending email to unintended recipients. However, it is useful to have a privacy disclaimer on all emails leaving the practice as an additional protection.

Document email in medical records

As with any communication, your process needs to ensure incoming emails are passed onto the appropriate person, actioned, documented in the patient's clinical record and managed in accordance with record-keeping requirements. Make sure your policy also addresses how clinical images sent to a practitioner, (for example as part of a telehealth consultation) will be used and stored. For more information please see Avant's factsheet: Storing, retaining and disposing of medical records.

Is email ever inappropriate?

Even if your patient consents to communication by email, there may be circumstances in which you are not comfortable emailing them the information. It may be particularly sensitive or detailed or need a complex explanation. It is always appropriate to exercise your clinical judgement to decline to send such information by email. You may consider a face-to-face consultation is necessary (in limited circumstances, telehealth may be suitable).

We would consider it inappropriate to deliver any bad news to a patient via electronic means.

You may also find that a patient responds to an email with further questions. Try to avoid back-and-forth conversations over email because there is a risk that these will turn into a chain of correspondence and you may find yourself providing medical advice without a proper consultation. In such situations, it is appropriate to decline to respond further via email and ask the patient to make an appointment.

Email link on your website

Delegate the task to an employee to monitor the emails being sent to the practice via the website email link. You can use keywords to block certain emails. For example, you could use a keyword filter such as 'test' that will result in the email being blocked and a message would be sent to the sender asking them to contact the practice to make an appointment.

Consider patient safety

Time-sensitive information

You can send time sensitive information by email, but you do need some safeguards in place to be sure the information has been received and actioned. You might ask the patient to acknowledge receipt of any email communication either by a generated 'read receipt' or a manual return email, depending on the sensitivity.

Urgent after-hours emails

Practices are not required to check email addresses 24 hours a day. However, you do need to be clear about how the account is being monitored, particularly if you publish the address anywhere, such as on your website. You could outline when email will be responded to and include an auto-reply advising how the address is being monitored and providing an appropriate emergency contact.

Additional resources

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

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

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

MJN372 06/20 (0983)