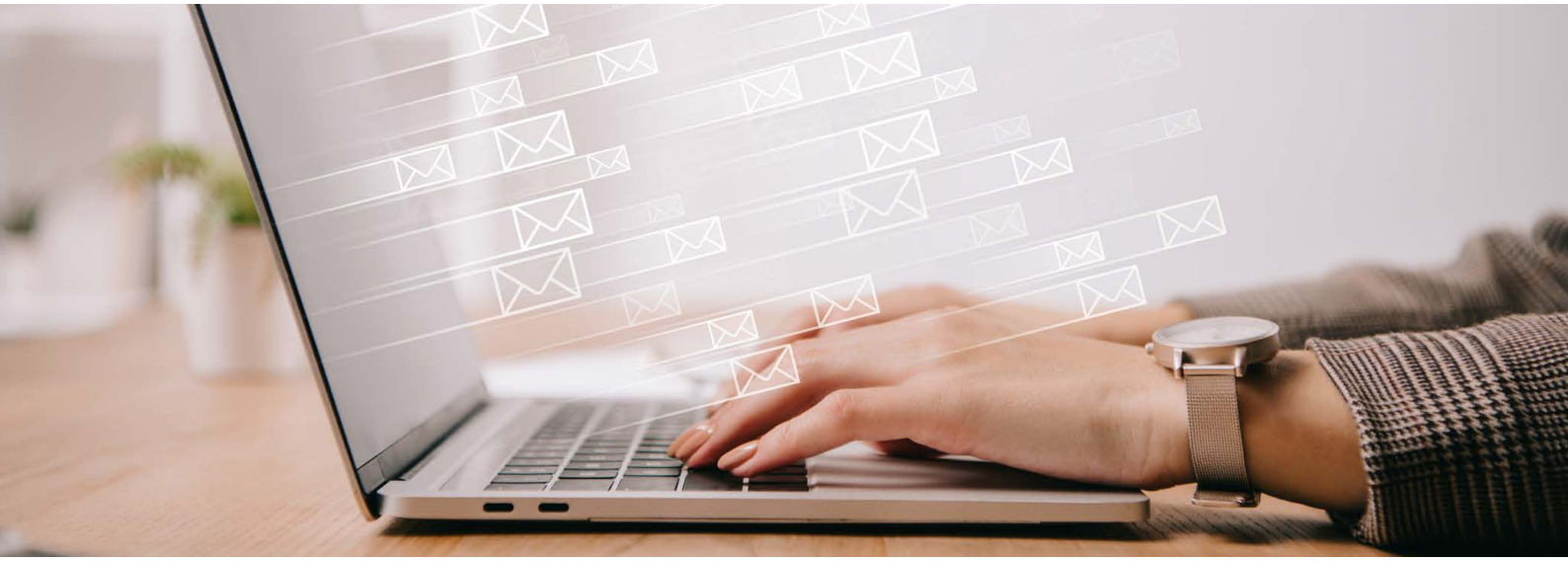
RACGP

Royal Australian College *of* General Practitioners

Healthy Profession.
Healthy Australia.

Fact sheet

Using email in general practice



This fact sheet provides information for general practices about using email to communicate health information with patients, health organisations, and third parties.

Can I use email to send healthcare information?

Email is one of the most prevalent and convenient forms of communication. GPs and general practices often receive requests from patients, other clinicians and third parties to send health information via email.

General practices must ensure their communication of health information is safe and secure. The use of unencrypted and unsecured email can create risks to the privacy and security of personal and sensitive health information.

Email can be used to communicate healthcare information but it is important general practices understand the risks and take steps to mitigate them before using email.

What are the risks of using email to send healthcare information?

All forms of written communication involve an element of risk that information could be read by someone other than the intended recipient. The risks of using unsecured or unencrypted email include:

- emails can easily be sent to the wrong recipient
- email is often accessed on portable devices, such as smart phones, tablets and laptops, which are easily lost or stolen
- emails can be forwarded or changed without the knowledge or consent of the original sender
- email is vulnerable to interception.

Because of the risks of email and fax communication, the RACGP has long been a strong advocate for the use of secure electronic communications as the most efficient and appropriate method of communication across the healthcare sector.

7272

What are my obligations under the Privacy Act 1988?

Health information is considered one of the most sensitive types of personal information. The Privacy Act 1988 (Privacy Act) provides extra protections around the collection, use or disclosure of health information.

Whilst the Privacy Act does not prescribe how healthcare organisations should communicate health information, reasonable steps must be taken to protect the information transmitted and the privacy of the patient. What is considered reasonable steps will depend on the nature of the information and the potential for harm caused by unauthorised access. Failure to take reasonable steps to protect health information may constitute a breach of the Australian Privacy Principles (APPs).

Assessing risk

Practices should consider the level of risk associated with how they use email to assist in determining the level of security needed in order to use email for communicating health information.

The diagram on the next page outlines different practice processes relating to email use and the level of risk they present. The diagram is intended for use as a general guide to highlight issues for GPs and general practices for further consideration when using email.

Further reading and links to policy and procedure templates

The use of secure electronic communication within the health care system
https://www.racgp.org.au/secure-electronic-communication

Information security in general practice
https://www.racgp.org.au/infosec

Privacy of health information
https://www.racgp.org.au/privacy

General practice policy and procedure templates Health information and medical research – OAIC
https://www.oaic.gov.au/privacy-law/privacy-act/health-and-medical-research

Privacy for health service providers – OAIC
https://www.oaic.gov.au/privacy/privacy-for-health-service-providers/

Secure messaging – The Australian Digital Health Agency
https://www.digitalhealth.gov.au/get-started-with-digital-health/what-is-digital-health/secure-messaging

Practice policies and processes risk assessement

High Risk

- Email communications are undertaken without the use of passwords or encryption.
- No formal policy or supporting resources are in place.
- No processes are in place to ensure email addresses are correct and are not sent to a generic inbox.
- No written consent from patient is obtained or recorded.

Medium Risk

- No written consent from patient is obtained or recorded.
- Email communications undertaken without the use of passwords or encryption.
- No processes in place to ensure email addresses are correct and are not sent to a generic inbox.

Low Risk

- Documented policies and resources exist.
- Consent from patient is obtained and recorded.
- Email address is verified by the practice before sending an email.
- Emails are sent with password protection OR email communications are sent using encryption software or via a secure website.

No Risk

- No email communication is used, or intended to be used.

Practice policies and processes explanation

- Emails may be sent to the wrong person or could be read by an unintended recipient.
- The use of unsecured and unencrypted email creates the risk that if the email is intercepted during transmission it can be easily be read.
- Unauthorised disclosure of healthcare information may have far-reaching consequences for the individuals impacted.
- The failure to protect healthcare information may result in action by the Office of the Australian Information Commissioner.
- When the practice has a policy in place regarding communications via email it guides practice staff on the appropriate use of email.
- When patients are provided with information about the risks of communicating healthcare information via unsecured and unencrypted email it enables them to provide informed consent. Patient consent to send information by email is recorded (for example, a note is made in the patient's record that a conversation has taken place).
- Emails sent with password protection OR email communications are sent using encryption software or via a secure website with passwords provided by another channel i.e. in person, phone or SMS, as they are much more secure.