



General practices should take reasonable steps to safeguard patient information when sending information to patients, health organisations or third parties by email, as with any other types of communication.

General practices should inform patients who request information to be sent by email, that there may be a risk (as with any other document) that it could be read by someone other than the intended recipient.

Background

General practices are increasingly receiving requests from patients, other clinicians and third parties for health information to be sent to them electronically because it is an easily accessible method of communicating.

The Australian Privacy Principles published by the Office of the Australian Information Commissioner state that: *“Health information is regarded as one of the most sensitive types of personal information. For this reason, the Privacy Act 1988 (Privacy Act) provides extra protections around its handling”.*

<http://www.oaic.gov.au/privacy/privacy-act/health-and-medical-research>

The Privacy Act defines health information as:

- a) information or an opinion about:
 - i. the health or a disability (at any time) of an individual; or
 - ii. an individual's expressed wishes about the future provision of health services to him or her; or
 - iii. a health service provided, or to be provided, to an individual; that is also personal information; or
- b) other personal information collected to provide, or in providing, a health service; or
- c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or
- d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Rationale

As all health information is sensitive by nature, all communication of health information, including via electronic means, must adequately protect the patient's privacy.

General practices should take reasonable steps to make their communication of health information adequately safe and secure. GPs, health providers and patients should be aware of the risks associated with using email in the healthcare environment.

Obligations under the Privacy Act

General practices must consider their obligations under the Privacy Act before they use or disclose any health information. The Privacy Act does not prescribe how a healthcare organisation should communicate health information. Any method of communication may be used as long as the organisation takes reasonable steps to protect the information transmitted and the privacy of the patient.

A failure to take reasonable steps to protect health information may constitute a breach of the Australian Privacy Principles and may result in action taken against the organisation by the Australian Privacy Commissioner. What amounts to reasonable steps will depend on the nature of the information and the potential harm that could be caused by unauthorised access to it. The RACGP has developed a matrix to assist practices in determining the level of security required in order to use email in general practice for communication.

Further information

Office of the Australian Information Commissioner's guidance "Chapter 11: APP 11 – Security of personal information".
<http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-11-app-11-security-of-personal-information>

For what should be included in an email policy see: The RACGP Standards for general practices (4th Edition) - specifically Criterion 1.1.2, 4.2.1, and 4.2.2, and the RACGP Computer Information and Security Standards (2nd edition) - specifically Standards 6 and 12.