Email and Texts to Patients

Electronic communication with patients (such as email or SMS) is convenient, cheap, and can make documentation easier. It can also create more work (with no reimbursement), be used inappropriately by patients, and raise privacy issues.

Defining email use

Your practice needs a written policy detailing:

- what information can be sent from the practice (appointment reminders? non-urgent recalls?)
- what information is appropriate for patients to send or request (change an appointment? seek clinical advice?)
- how patient consent is gained and documented
- how messages and responses are recorded in the patient's record
- who is responsible for monitoring incoming messages
- the acceptable period of time for the practice to respond to messages
- use of professional language, e.g. not emoticons or word-abbreviations such as "CU" for "see you"
- the IT security safeguards in place.

Patient consent

Patients should give consent to be contacted by email or SMS – preferably in writing. This could be done when new patients supply their details or when current patients confirm an appointment. When consenting, the patient should understand:

- what type of information can be sent
- whether the practice is encrypting email and, if not, that email messages are not secure
- that they can opt out
- that they should notify the practice of a change of email address or phone number.

If a patient does not want to use email or SMS, procedures should be in place to accommodate this.

Managing patient expectations

An automatic reply to incoming emails can be set up, for example:

Please note that this email address is checked by practice staff x times a day. Please do NOT email medical or clinical questions to us – for all enquiries please call us on (02) 1234 5678.

We do not use encrypted email and cannot guarantee confidentiality of information sent by email.

If a patient uses email inappropriately, e.g. asking a clinical question when the practice has decided not to answer clinical questions by email, a polite response should be provided, such as:

To provide the best care to our patients, we do not answer clinical questions by email. Please call us on (02) 1234 567 to make an appointment.

All efforts to contact the patient must be made and documented if a patient's email or SMS indicates that urgent medical attention is needed.

Privacy and security

The practice's use of email and SMS should be included in the practice's privacy policy.

An email may be seen by a patient's family, friends or colleagues. It may be inadvertently sent to the wrong email address; it may even be hacked into or posted on the internet with worldwide exposure.

The consequences of a privacy breach depend on the sensitivity of the information – appointment times are very different from psychiatric illness details, for instance. Consider carefully what information you include in electronic communications.

Confirm a patient's identification and contact details before hitting "send".

Australian privacy law requires organisations to take reasonable steps to protect the security of personal information they hold. "Reasonable steps" may include:

- robust IT systems – firewalls, virus protection, frequent password updates, backups, maintenance of hardware and software
- procedures – appropriate staff access levels, safe use of internet, staff sign confidentiality agreements, currency of contact details regularly checked
- building security and alarms.

Encryption or secure messaging provides greater email security but this is not currently a legal requirement for medical practices.

If your email service is backed up to the cloud and the servers are not located in Australia, you will need to comply with specific privacy law about this (APP8).

Resources

Office of the Australian Information Commissioner. Australian Privacy Principles. Available at **oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles**