Dr Eliza Malkoun

P: (02) 4243 9211 F: (02) 4243 9212

61 Auburn St Wollongong, NSW, 2500

Provider number 411336BK

E: admin@emmedical.com.au

EM Medical Communication Policy

Email, SMS, Internet and Social Media

Current as of: November 2021

This document is a guide only and is to be followed subject to the judgment of the user. Whilst all care has been taken in its preparation, the distributor will not be held liable for any losses or damage that may occur in applying the information contained within the document. The distributor assumes no responsibility for the contents of any websites listed.

General practices are increasingly using electronic communication to correspond with patients and other health professionals.

Our practice electronic communication policy for use with email, SMS, internet and social media will help protect the security of patient information and the reputation of EM Medical.

The practice team will be familiar with the following policy, comply with the policy, and understand the risks associated with using electronic forms of communication, both internally and externally.

The Electronic Communication Officer

The practice has appointed Erin Bozinovski, Practice Manager to act as Electronic Communications Officer.

The Electronic Communications Officer is responsible for:

- Maintaining this policy.
- Providing an information session on this policy as part of a new employee's induction.
- Informing staff of updates and refresher training through staff meetings and notices.
- Responding to any concerns that staff or patients have with the policy.
- Implementing and recording quality improvements to the system as a quality improvement activity in the Practice Improvement Log.

Email and SMS – For staff

The use of email and short message services (SMS) are recognised as a useful tool for communication purposes. Practice staff are permitted to use the practice email accounts to send and receive business related material such as education updates, stakeholder communication, submitting Medicare provider number applications and communicating with locums or other staff where appropriate.

Practice staff will have access to a practice email account in the following levels:

- **Generic:** This is the address that patients can utilise to contact the practice, for example admin@emmedical.com.au
- **Practice manager:** Personalised use of a practice email account
- **Clinical practice team members:** Medical practitioners, nurses, allied health practitioners will have personalised use of a practice email account

The use of the practice email account is for business communications only.

Patient information will only be sent via e-mail if it is securely encrypted according to industry standards, practice policy and where the patient has consented to this mode of direct communication. Employees are reminded that the practice may become liable for the contents of any email message under certain circumstances. As such, a template email disclaimer will be inserted into the signature of all practice emails.

The use of personal email accounts using practice internet and computer systems is may be used in personal/lunch/break times where this does not interfere with day to day operations. Large files such as video files and photographs should not be transmitted over the practice internet computer systems for personal communication.

Protection against spam and theft of information

Staff will need to exercise caution in email communication and are advised to:

- Not open any email attachments or click on a link where the sender is not known.
- Not reply to spam mail.
- Not to share email passwords.
- Never try to unsubscribe from spam sites.
- Remain vigilant: do not provide confidential information to an email (especially by return email) no matter how credible the sender's email seems (for example, apparent emails from your bank).
- Be aware of phishing scams requesting logon or personal information (these may be via email or telephone).

Encrypted files are not automatically checked for viruses. All team members are to save, decrypt and then scan before opening the document.

Password maintenance

Each of our team members will have unique identification for all protected systems.

Staff will not share passwords. Access will be by individual password only and passwords will be periodically changed and immediately if compromised.

- Passwords will not be generic.
- Passwords will be private and not shared.
- Passwords cannot be re-used.
- Passwords will be made up of 6 – 8 characters with alpha, numeric and special characters. The preference is use of a unique phrase.
- Our staff are strongly discouraged from using:
  - Dates of birth.
  - Family or pet names.
  - Dictionary words.

Password management

- Only the Electronic Communications Officer or practice manager can reset passwords.
- User identifications are archived or removed upon leaving the employment of the practice.
- Lock-out will occur after three unsuccessful login attempts to an account.

Email and SMS – For patients

Our patients will be given the option of being contacted by electronic means such as via email and/or SMS.

All new and existing patients in the practice will be given an information sheet on our electronic communication policy, and are asked to provide signed consent to agree or disagree to be communicated with in this manner.

It is acknowledged by the practice that consent is implied if the patient initiates electronic communication with the practice.

Reception staff are to check each patient has this information on their record on arrival to the practice, along with the verification of their name, date of birth and address.

The signed consent will be scanned and recorded in the patient electronic record and their response recorded on the practice software.

The consent form will state that the practice may use this mode of communication:

- to send reminders for a scheduled appointment.
- when the patient needs to make an appointment to review a test result.
- as a reminder that a generic preventative screening test (for example, flu vaccine, skin-check, cervical screening) is due.

Further information will state that the practice:

- cannot guarantee confidentiality of information transferred via email (if using encryption, please state how your encryption works).
- will comply with the Australian Privacy Principles and the Privacy Act 1988.
- communications will not contain sensitive information, due to the risk of confidential information being accessed inadvertently or intentionally by a third party.

- communications will not contain results that only the general practitioner should be divulging in a follow-up appointment, ie abnormal results, education concerning a new diagnosis, etc
- communication will not entail promotion of any product and/or preventative health care (as some patients can interpret this as an advertisement)

Patients will be advised through the consent form that:

- emails will be answered as soon as possible depending on urgency.

patients should not use email to contact the practice in an emergency

Our practice email account for patients and stakeholders for non-urgent communication with our practice is admin@emmedical.com.au

This email account will the routinely checked throughout the business day by the delegated authority, Erin Bozinovski, Practice Manager

- at the start of business
- midday
- one hour before end of business

The email message will then be forwarded to the appropriate team member for response. Communication conducted with a patient via electronic means will be added to the patient's medical record by the team member resolving the enquiry.

When recalling a patient for a test result, the extent to which patients are followed up will depend on the level of urgency and the clinical significance of their test results. If the patient has not responded to the SMS or email then other forms of communication (phone call, registered mail) will be considered.

Email and SMS between the practice and the patient will form part of the medical record and need to be included, as must any actions taken in response to the message.

Internet

The use of the internet as a legitimate business and research tool is both recognised and approved by EM Medical. However, staff and management have a responsibility to ensure that there is no abuse of the resources for private purposes, that staff productivity is not compromised, that offensive material is not spread throughout the organisation and that the practice computer system is protected from the introduction of computer viruses.

All downloads from the internet must be scanned for viruses.

All sites accessed must comply with legal and ethical standards and the practice policies. The internet must never be used to download or access any illegal software or pornographic, defamatory, offensive, share-trading or gambling-related material.

Downloading of material via the internet slows access for other staff. The internet should not be used for downloading music, videos or radio programs, for making personal purchases or accessing interactive social websites, including Facebook, YouTube, Skype and Twitter, except in a professional capacity and approved by the Electronic Communications Officer.

Web browser security settings are not to be changed without authorisation of the practice manager.

The practice will have in place firewalls and intrusion detection systems as advised by our IT company IT&T.

Social media

Social media is defined as websites and applications that enable users to create and share content or to participate in social networking. These include Instagram, Facebook, Twitter and YouTube. This practice does not participate in any social media.

Social media is not permitted to be used from practice devices in a private capacity by any staff member.