Vitality Solutions
Electronic Communication Policy

Preamble

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

Our practice electronic communication policy for use with email and SMS will help protect the security of patient information and the reputation of Vitality Solutions.

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.

This email policy is adapted from and in accordance with RACGP 5th Edition standards and AHPRA guidelines.

Clinical information between Health Providers

Communication of clinical information to and from healthcare providers are completed from within the practice's clinical software, wherever possible, using a secure clinical messaging system such as Medical Objects.

The use of a practice's clinical software means that a record of communication is automatically retained in the patient's medical record. **This is not possible when communicating with patients.**

Email and SMS – For patients

All new and existing patients in the practice will be given a practice information sheet and are asked to provide signed consent to agree or disagree to be communicated with in this manner via our New Patient Information Form or Update of Details Form.

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.
- 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, i.e., abnormal results, education concerning a new diagnosis, etc.

Email communication or replies received from our automated reminders is not our preferred method of communication from patients as it is not secure and does not meet the required standards. Any emails or replies received for patient related enquiries, will not be actioned by reception.

Patients will be advised through the consent form, by automated email or SMS reply and via our website that:

- Emails and SMS generated through our system are not routinely monitored.
- Patients should not reply to system generated SMS use email or to contact the practice:
    - In an emergency.
    - To book or cancel an appointment.
    - To request scripts, referrals or any other services from the practice.

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 in one week, then other forms of communication will be considered.

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

General protection

If any information held in our email accounts that is specific to a patient's health information will be downloaded as per practice policy. It will be imported into relevant patient file to ensure contents are backed up with the rest of our data.

- We do not provide confidential information to an email address (especially by return email) no matter how credible the sender's email seems (e.g., apparent emails from your bank).
- Use a spam filtering program.
- Encryption of patient information
- All email communications should be treated as confidential.
- When sending patient information or other confidential data by email, it is best practice to use encryption.
- Be aware that encrypted files are not automatically checked for viruses. They have to be saved, decrypted and then scanned for viruses before being opened.

Password maintenance

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

Staff will not share passwords. Clinical 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.
- Our staff are strongly discouraged from using:
    - Dates of birth.
    - Family or pet names.
    - Dictionary words.

Password management

- Only the I.T. Support 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.

The Electronic Communication Officer

The practice has appointed our 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 useful tools 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: info@vitalitysolutions.com.au
- Practice manager: admin@vitalitysolutions.com.au

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

Patient information will be sent via e-mail according to industry standards, practice policy and where the patient has consented to this mode of direct communication.

We send two different types of emails from our system:

1. Unsecure:

   These emails are not secure and can be seen without any further steps or authentication. We use these types of emails for any information-based patient handouts as well as any other contact that doesn't have patient information included.

   Unfortunately, if you ask for any test results or correspondence to be emailed to you from your patient file, it will be sent via this method. You must be aware that there are risks involved in requesting information this way as emails can be hacked and information received in the data can be used for other purposes.

2. Secure:

   We utilise additional security features for any emails that we sent which include your personal information, where possible.

   These emails will provide a link for you to click on and will ask you to send a code to the phone number we have on file to 'unlock' the document we have sent you.

Protection against spam and theft of information

The practice utilises a spam filtering program.

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).