Electronic Communication Policy

1.1.1. Policy

General practices are increasingly using electronic communication to correspond with patients and other health professionals. Our practice's electronic communication policy for use with email, SMS, internet and social media will help protect the security of patient information and the reputation of Eastbound Medical Clinic. 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 external.

1.1.2. The Electronic Communication Officer

The practice has appointed the Communication Officer/Advisor as the 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.

1.1.3. 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:** reception@eastboundclinic.com.au
- **Practice manager:** manager@eastboundclinic.com.au
- **Receptionists**: Group email, receptionists@eastboundclinic.com.au
- **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 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.

This message is confidential and should only be used by the intended addressee. If you were sent this email by mistake, please inform us by reply email and then destroy this message. The contents of this email are the opinions of the author and do not necessarily represent the views of Eastbound Medical Clinic.

The use of personal email accounts using practice internet and computer systems is not permitted**.** Large files such as video files and photographs should not be transmitted over the practice internet computer systems for personal communication.

1.1.4. Protection against spam and theft of information

The practice utilises a spam filtering program **SpamTitan utilised by the practices IT support service.**

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).
- Forward any suspicious emails to IT support team for assessment – support@gpsupport.com.au

1.1.5. Password Maintenance

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

Access will be by individual password only and passwords will be if compromised.

- Passwords will not be generic.
- Passwords will be private and not shared.

1.1.6. 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 patients in the practice will be given an information on our electronic communication policy via our registration form, 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 registration forms states that the practice may use this mode of communication:

- To send reminders for a scheduled appointment.
- When the patients results are clinically clear and no action is required.
- 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. E.g. Mental Health Care Plans.
- 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.

Our practice email account for patients and stakeholders for non-urgent communication with our practice is **reception@eastboundclinic.com.au**

This email account will the routinely checked throughout the business day by the reception team members on duty:

- 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.

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.

The practice email has an automated response to advise patients to contact the clinic by telephone if requiring immediate response.

Automated Reception email response:

Subject line: Thanks for getting in touch.

Hi,

Thank you for your email. This is an auto-reply message.

We received your email and will get back to you with a response as soon as a member of our reception team is available. If your email requires immediate action, please call our reception team

on 9579 3522. In the case of an emergency, please call 000 or go to your nearest Emergency Department.

Regards,

Eastbound Medical Clinic
Specialist Family Physicians

P. (03) 9579 3522 www.eastboundclinic.com.au
F. (03) 9563 8765 179 EAST BOUNDARY ROAD, EAST BENTLEIGH. VIC. 3165

1.1.7. Electronic Communication – Emailing Patients

As a general rule the Eastbound Medical clinic will not email patients personal health information such as referrals, medical certificates and results. The only occasion emails can be sent to a patient is if a patient specifically requests it and all alternative methods of communication (fax and post) have been declined.

In the instance that a patient requests personal health information to be emailed the following requirements must be reviewed:

- We will not communicate with Hotmail accounts
- We will not email highly sensitive health information i.e. Mental Health Care Plans

If the above points are met the patient must be read out the following template to ensure the patient is able to provide informed consent.

The use of unencrypted and unsecured email can create risks to the privacy and security of personal and sensitive health information. Eastbound Medical does not believe it to be a safe and secure method of communication. All forms of electronic communication involve an element of risk that information could be read by someone other than the intended recipient.
Consenting to receiving personal health information via email confirms you understand the associated risks when using unencrypted and unsecure email. I do also need to let you know your consent will be documented on your patient file.
Do you provide verbal consent?

Reception is responsible for documenting the patients response in the patient's Medical Director file.

1.1.8. Internet

The use of the internet as a legitimate business and research tool and is recognised and approved by Eastbound Medical Clinic. 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, GP support.

1.2. Using social media in our practice

1.2.1. Policy

Social media is defined as online social networks used to disseminate information through online interaction.

Regardless of whether social media is used for business related activity or for personal reasons, the following standards apply to members of our practice team, including general practitioners. Practitioners and team members are legally responsible for their postings online. Practitioners and team members may be subject to liability and disciplinary action including termination of employment or contract if their posts are found to be in breach of this policy.

All members of our practice team must obtain the relevant approval from our social media officer prior to posting any public representation of the practice on social media websites. The practice reserves the right to remove any content at its own discretion.

Any social media must be monitored in accordance with the practice's current polices on the use of internet, email and computers.

1.2.2. Procedure

Our practice has appointed our Communications Officer/Advisor with the designated responsibility to manage the practice's social media. All posts on the practice's social media websites must be approved by this person.

1.2.3. Staff Conduct

When using the practice's social media, all members of our practice team will not:

- Post any material that:
  - Is unlawful, threatening, defamatory, pornographic, inflammatory, menacing, or offensive
  - Infringes or breaches another person's rights (including intellectual property rights) or privacy, or misuses the practice's or another person's confidential information (e.g. do not submit confidential information relating to our patients, personal information of staff, or information concerning the practice's business operations that have not been made public)
  - Is materially damaging or could be materially damaging to the practice's reputation or image, or another individual
  - Is in breach of any of the practice's policies or procedures
- Use social media to send unsolicited commercial electronic messages, or solicit other users to buy or sell products or services or donate money
- Impersonate another person or entity (for example, by pretending to be someone else or another practice employee or other participant when you submit a contribution to social media) or by using another's registration identifier without permission
- Tamper with, hinder the operation of, or make unauthorised changes to the social media sites
- Knowingly transmit any virus or other disabling feature to or via the practice's social media account, or use in any email to a third party, or the social media site
- Attempt to do or permit another person to do any of these things:
  - Claim or imply that you are speaking on the practice's behalf, unless you are authorised to do so
  - Disclose any information that is confidential or proprietary to the practice, or to any third party that has disclosed information to the practice
- Be defamatory, harassing, or in violation of any other applicable law
- Include confidential or copyrighted information (e.g. music, videos, text belonging to third parties)
- Violate any other applicable policy of the practice.

1.2.4. Testimonials

Our practice complies with the Australian Health Practitioner Regulation Agency (AHPRA) national law, and takes reasonable steps to remove testimonials that advertise our services (which may include comments about the practitioners themselves).

Our practice is not responsible for removing (or trying to have removed) unsolicited testimonials published on a website or in social media over which we do not have control.

1.2.5. Personal Social Media Use

Any social media posts by members of our practice team on their personal social media platforms should:

- Staff are free to personally engage in social media outside of work hours, as long as their actions do not have the potential to bring the practice into disrepute. Employees may not represent personal views expressed as those of this practice.
- Any social media posts by staff on their personal social media platforms must not reveal confidential information about the practice or a person who uses the practice (e.g. staff should not post information relating to patients or other staff, or information concerning the practice's business operations that have not been made public).
- Include the following disclaimer example in a reasonably prominent place if they are identifying themselves as an employee of the practice on any posting: '*The views expressed in this post are mine and do not reflect the views of the practice/business/committees/boards that I am a member of*', and
- Respect copyright, privacy, fair use, financial disclosure and other applicable laws when publishing on social media platforms.

Social media activities internally and externally of the practice must be in line with this policy.