Gardens Medical Group Email Policy

Policy Title: Email Communication Policy
Review Date: September 2027
Approved By: Jenny Edwards CEO/Practice Manager

---

1. Purpose

This policy outlines the appropriate and secure use of email communication in the transmission and receipt of healthcare information at Gardens Medical Group.
It ensures compliance with the RACGP Standards for General Practices (5th Edition), the Privacy Act 1988, and the Australian Privacy Principles (APPs) to protect the privacy and confidentiality of patient information.

---

2. Scope

This policy applies to all staff, contractors, and healthcare providers working within Gardens Medical Group who use email to communicate internally or externally with patients, healthcare organisations, or third parties.

---

3. Policy Statement

Gardens Medical Group recognises that email is a convenient form of communication, but also carries inherent risks.

The practice will take reasonable steps to protect personal and sensitive health information transmitted via email and will use secure methods wherever possible.

Email may be used to communicate health information only when the risk has been assessed and appropriate safeguards are in place, including obtaining informed consent from the patient.

---

4. Definitions

- **Secure Messaging:** An encrypted, standards-based method of electronic communication between healthcare providers.
- **Unencrypted Email:** An email sent through a standard email system (e.g., Outlook, Gmail) without encryption, considered insecure.
- **Encryption:** The process of converting information into a secure format to prevent unauthorised access.
- **Reasonable Steps:** Measures proportionate to the sensitivity of the information and potential risk of harm.

---

5. Acceptable Use

5.1 Internal Email

- Practice staff may use internal email for administrative and operational purposes.
- Sensitive health information should not be sent via internal email unless encrypted or within a secure clinical software system.

5.2 External Email (Patients, Health Organisations, Third Parties)

- Secure messaging (e.g., Argus, HealthLink, Medical-Objects) is the preferred method of communication between healthcare providers.
- Emails containing patient health information must:
  - Be sent only when secure messaging is unavailable or unsuitable.
  - Be encrypted or password-protected.
  - Include a disclaimer stating the confidential nature of the information.
  - Be sent to a verified email address.
- Staff must verify the recipient's email before sending and ensure it is not a generic or shared address.

---

6. Patient Consent

- Patients must be informed of the risks associated with email communication, including that unencrypted emails may not be secure.
- Informed consent must be obtained and recorded in the patient's file before sending any personal health information by email.
- Consent can be obtained:
  - In writing (e.g., email consent form)
  - Verbally (documented in the patient's notes)
- Consent should specify:
  - The patient's preferred email address
  - The type of information that may be sent
  - Any limitations (e.g., no sensitive or diagnostic results via email)

---

7. Security Measures

To minimise risks, the following measures must be applied:

- Use password-protected or encrypted attachments when sending health information.
- Passwords must be communicated separately (e.g., by phone, SMS, or in person).
- Practice computers and devices must have:
  - Updated antivirus software
  - Strong password protection
  - Automatic screen locks
- Email accounts must not be accessed from public or shared computers.
- Practice email systems must be protected with multi-factor authentication (MFA**)** where available.

---

8. Verification and Accuracy

Before sending an email:

- Confirm the correct recipient email address.
- Confirm spelling and accuracy of the address.
- Ensure attachments are correct and necessary.
- Avoid including unnecessary patient identifiers.

---

9. Confidentiality and Record Keeping

- All emails containing clinical information form part of the patient's health record and must be uploaded or copied into the clinical software.
- Staff must ensure sensitive information is not retained in personal inboxes.
- Deleted emails must be removed from 'deleted items' regularly in accordance with the practice's record management policy.

---

10. Breach of Privacy or Security

If an email containing patient information is sent to the wrong recipient or accessed by an unauthorised person:

- The incident must be reported immediately to the Practice Manager.
- The practice will:
  - Take steps to mitigate harm,
  - Notify affected individuals, and
  - Report the breach to the Office of the Australian Information Commissioner (OAIC) if required.

---

11. Training and Awareness

- All staff must complete annual privacy and information security training.
- Staff will be trained on:
  - Identifying and managing risks associated with email communication
  - Procedures for obtaining patient consent
  - Secure use of email and password protection

---

12. Disclaimer

All outgoing external emails containing health information must include the following disclaimer:

Confidentiality Notice:
This email and any attached files are confidential and intended solely for the use of the individual or

entity to whom they are addressed. If you are not the intended recipient, please notify the sender immediately and delete this email. Unauthorised disclosure, copying, or distribution is prohibited. Please note that email communication may not be secure. If you do not wish to receive correspondence via email, please inform our practice.

---

13. Review

This policy will be reviewed every two years or sooner if there are:

- Changes to legislation,
- Updated RACGP guidance, or
- Technological or operational changes in communication methods.

---

14. References

- RACGP: *Information security in general practice*
- RACGP: *Privacy and managing health information in general practice*
- RACGP: *Position statement – Safe and effective electronic transfer of information*
- OAIC: *Guide to health privacy*
- OAIC: *Australian Privacy Principles (APPs)*
- Australian Digital Health Agency: *Secure Messaging*