THE BOMBALA STREET SURGERY

62 Bombala Street, Cooma 2630 **Phone (02) 64525888**
P.O. Box 650 Cooma 2630 NSW ABN 76 305 349 635 **Fax (02) 64524868**

SMS Communication

2.1 Authorisation Requirements

SMS communication is used with patient consent. Authorisation includes:

- Patient signature on the New Patient Registration Form (scanned to patient file, if applicable).
- Confirmation of mobile number at each visit.
- Explicit SMS consent via:
  - HotDoc confirmation
  - Practice Management Software entry

2.2 SMS Content and Usage

- SMS messages **do not include sensitive health information** (e.g., pathology results).
- SMS reminders are used for:
  - Appointment confirmations
  - Health recalls
  - General reminders (e.g., immunisations, check-ups)

2.3 Record Keeping and Tracking

- SMS sent via HotDoc is recorded in the HotDoc account.
- SMS sent via Practice Management Software is automatically recorded in the patient file.
- The system:
  - Records the reminder in the patient file
  - Allows review of SMS reminders and patient responses
  - Supports follow-up for recalls where no response is received

---

3. Email Communication

3.1 Approved Email Use

- Only practice-provided or secure health network emails (e.g., *@practicename.com.au*, HealthLink) are permitted.
- **Personal email accounts must not be used** for any work-related or patient communications.

3.2 Professional Standards

- Maintain a clear, respectful, and professional tone.
- Use a standardised email signature including:
  - Name and role
  - Practice contact details
  - Confidentiality disclaimer

3.3 Patient Communication via Email

Email is permitted **only with patient consent**, which must be documented in the clinical record.

- **Not suitable for urgent issues**
- If sensitive/personal information must be sent:
  - Use encrypted or secure messaging services.
  - Use minimal identifiers if encryption is unavailable.
  - Inform the patient of potential risks and obtain acceptance.

3.4 Security and Privacy

- Confirm recipient email addresses before sending.
- Attachments with sensitive information must be:
  - Password-protected or encrypted
- Ensure strong password security on email accounts and devices.
- Do not leave devices unattended while logged in.

---

4. Inappropriate Use of Email

Strictly prohibited:

- Sending or forwarding offensive, defamatory, or discriminatory content.
- Sharing passwords or login credentials via email.
- Using practice email for personal or unrelated business matters.

---

5. Documentation and Record Retention

- All clinical or patient-related emails must be:
  - Saved in the patient's Electronic Health Record (EHR)
- Retain according to:
  - NSW Health Records Act
  - Medical Board of Australia guidelines

---

6. Monitoring and Access

- The practice may monitor and audit email accounts to ensure compliance.
- Monitoring is conducted under relevant workplace surveillance and privacy laws.

---

7. Staff Training

All staff must complete:

- Onboarding and **annual training** on:
  - Privacy and confidentiality
  - Appropriate electronic communication
  - Email-related security risks

---

8. Breaches and Consequences

Policy violations, especially unauthorised health data disclosures, may result in:

- Disciplinary action
- Notification to the **Office of the Australian Information Commissioner (OAIC)**
- Notification to **AHPRA** (if applicable)