

**STANDARD 4.2 MANAGEMENT OF  
HEALTH INFORMATION**

## **Criterion 4.2.2 Information security**

---

The security of patient health information in our practice is maintained.

### **Indicators**

- ⌘ A. Patient health information in our practice is neither stored nor left visible in areas where members of the public have unrestricted access, or where constant staff supervision is not easily provided (interview, direct observation).
- ⌘ B. Our facsimile machines, printers and other communication devices are only accessible to authorised staff (direct observation).
- ⌘ C. Our GP(s) and staff can describe how they ensure security of patient health records (interview).
- ⌘ D. If our practice uses computers to store patient health information, our practice ensures that:
  - our GP(s) and staff have personal passwords to authorise appropriate levels of access to health information
  - screensavers or other automated privacy protection devices are enabled
  - backups of electronic information are performed at a frequency consistent with a documented information disaster recovery plan
  - backups of electronic information are stored in a secure offsite environment
  - antivirus software is installed and updated
  - all internet connected computers have hardware/software firewalls installed (document review).
- ⌘ E. If our practice uses computers to store personal health information, our practice has an information disaster recovery plan that has been developed, tested and is documented (document review).