CARD 4

Security of information

1. Keeping information secure
Protection is needed against both external threats such as theft and internal threats such as inappropriate access by staff. Health professionals should not leave computers, medical records or files unattended in the workplace. Ideally, all records and laptops should be kept in a locked environment. Health professionals should not normally take records or laptops containing electronic information out of the workplace. Where this cannot be avoided, for example if it is necessary to take records on visits to patients’ homes, procedures for safeguarding the information should be in place. Discussion about clinical management of patients should be kept confidential and out of earshot of those not involved in their care and especially the public. All people who come into contact with personal health information in their work should have training in confidentiality and security issues.

Health professionals who are also employers should ensure that employees are aware of their ethical, legal and contractual duty of confidentiality and how to keep information secure within their health setting. (See also Card 1: ‘Security’.)
2. **All records**

For all types of records health professionals should:
- never inappropriately access records
- shut/lock doors, offices and filing cabinets
- wear ID if issued
- query the status of visitors/strangers
- not tell unauthorised personnel how the security systems operate
- advise senior personnel if anything suspicious or worrying is noted
- confirm the identity of telephone callers.

3. **Manual records**

Manual records should be:
- held in secure storage
- booked out from their normal filing system
- tracked if transferred, with a note of their current location within the filing system
- returned to the filing system as soon as possible after use
- stored closed when not in use so that the contents are not seen by others
- inaccessible to members of the public
- kept on site unless removal is essential.

4. **Electronic records**

In the case of electronic records health professionals should:
- always log out of any computer system or application when work is finished
- not leave a terminal unattended and logged in
- not share Smartcards or passwords with others
- change passwords at regular intervals to prevent others using them
- always clear the screen of a previous patient’s information before seeing another.
5. **Email and fax**
In the case of email and fax:
- health professionals should be satisfied that there are appropriate arrangements for the security of personal information when it is stored, sent or received by fax, computer, email or other electronic means
- whenever possible, clinical details should be separated from demographic data
- all data transmitted by email should be encrypted
- when information is being transmitted by fax, it is sensible to enquire whether the receiving machine is in a publicly accessible area, such as a waiting room, or in a private office, as information must only be transmitted when the receiving machine is known to be secure both during and out of working hours. Wherever possible, it should be confirmed after transmission that the intended recipient has collected the information. Where it is necessary to transmit particularly sensitive patient information to other health professionals, it may be appropriate to consider other, more secure, means of communication. (See also Card 1: ‘Contracting’.)

6. **Data retention and disposal**
The health departments give detailed advice about the minimum retention periods applicable to NHS records. The recommendations apply to both electronic and manual records, and the BMA advises private practitioners to follow the same rules. When health professionals are responsible for destroying health records, they must ensure that the method of destruction is effective and does not compromise
confidentiality. Incineration, pulping and shredding are appropriate methods of destroying manual records. Electronic data should be destroyed using appropriate data destruction software. (See also Card 1: ‘Records Management’.)