Data protection

Chris Davies explains why compliance should be a priority for every practice.

The key legal requirement for processing personal information is the Data Protection Act 1998. The authority responsible for data protection in the United Kingdom is the Information Commissioner's Office (ICO) which has extensive powers of enforcement. Consequently, punishment for breaches of the act can severely inhibit a practice's ability to carryout its day to day business. For example, the ICO can order a practice to completely cease processing all personal data.

For the purposes of the act, 'processing' includes almost everything done with information whether it exists physically or on a computer. Therefore, if you handle and store information about an identifiable, living person you are legally obliged to protect that information. For dental practices this means that information held about patients and employees needs to be dealt with cautiously. Broadly, to ensure compliance with the act a practice should:

- Only collect information that it needs for the purpose of running the practice.
- Keep information secure and confidential.
- Ensure that information is relevant and up to date.
- Only hold as much information as it needs, and only for as long as it needs it.
- Allow the subject of information to see it upon request.

Chris Davies
is a partner at JCP Solicitors.

It's important to keep your patients' data secure

In addition, most dental practices also need to notify the ICO that it is a data controller. This is a legal requirement and failure to do so is a criminal offence. Furthermore, where a practice is entirely or partly funded by the NHS, additional legal obligations exist. Of these, the most significant is the Freedom of Information Act which imposes extra restrictions on the practice in relation to the information it handles as a public organisation.

Keeping patient records

In order to ensure compliance, patient records should be recognised as a specific responsibility within every dental practice. Patient records of all types and formats, including electronic records, should be held in a way so that they are secure and confidential. In addition, the patient record system should enable the efficient retrieval of information when it is needed and where patient records are held in a digital format, regular back-ups should be scheduled.

Destroying patient records

The British Dental Association provides guidelines for the retention of patient records in community dental practices. These are:

- 11 years for adults; and
- 11 years for children, or up to their 25th birthday (whichever is the longer).

When patient records have reached the end of their administrative life, they should be destroyed in a secure manner. This can be undertaken on site or via an approved contractor. Where a contractor is used, the practice should ensure that the contractor signs a confidentiality agreement and provides a written certificate as proof of destruction.

On rare occasions, where a patient record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place.