Briefing

Record storage

Accurate and clear records are essential to allow practitioners to communicate and monitor the progression of treatment

Practitioners have a professional obligation to keep records and store them securely. There are a number of legal rules, regulations and principles that relate to the storage of patient records and there are many practical steps practitioners can take to ensure their compliance with those rules.

The College of Podiatry Standard 1 – Record Keeping sets out practical steps that practitioners should be mindful of when approaching the storage of records:

- A comprehensive information security policy should be in place with all staff aware of their obligations under that policy and regular data protection training to ensure the practice is complaint with data regulations.
- Patient records should be stored securely within lockable cabinets (which remain locked when not in use) and returned to the filing system as soon as possible after use. When in clinic, the records should be positioned so that no one can read or access them other than the practitioner and the patient that the records relate to.
- Any computer or electronic device that holds records should have robust access controls e.g. password controlled access.
- The software program or system that is used to store patient records should have robust access controls e.g. password controlled access.
- The practitioner should log out of any system when they are finished and should not leave a monitor logged in and unattended.
- Passwords and log ins should not be shared or otherwise be made accessible e.g. written on post-it notes.
- When undertaking home visits the practitioner should be aware that records should not be left ‘on show’ or unsecured (for example they could be placed in a locked box in the boot of the car).
- When discussing a patient the practitioner should be careful not to do so where they could be overheard and should avoid using identifying information where possible.
- Caution should be taken when practitioners use their own electronic storage devices. A policy should be in place and the ability to lock/wipe the device remotely should it be lost or stolen is desirable.

In the event that records are to be shared either with the patient by way of a subject access request or disclosed to a firm of solicitors or the police it is essential that the identity of the requestor and their authority to make the request is clear, any necessary consents are obtained and that the information is reviewed prior to disclosure to remove any irrelevant information. The information should be sent securely.

The Information Commissioner’s website provides a huge amount of guidance: https://ico.org.uk/ and guidance can be sought from the College.

Contact

Keara Bowgen-Nicholas
Solicitor, Healthcare Professionals
E. kear-bowgen-nicholas@rlb-law.com
T. 029 2034 8721