

Blyth Family Dental Practice Records Management Policy

This dental practice holds and maintains information about the business and its patients that is necessary for the efficient running of the practice and the effective provision of dental care. This policy describes the information that must be kept, how it must be stored, archived and disposed of to ensure that the practice complies with the requirements of data protection legislation.

The practice **Confidentiality policy** describes the need for all members of the dental team to keep patient information confidential and practice procedures for handling information about patients; it must be followed always. The arrangements for keeping information safe are described in the practice **Data security policy**, which includes the measures for physical and electronic security.

The practice Privacy Notice for patients helps them understand how the practice uses and protects their personal information.

Retaining information

Information about the business and its patients is kept for no longer than required.

- **Patient records** are maintained and kept up to date while the individual remains a practice patient. When they cease to be a patient of the practice, their records are retained for ten years following their last visit to the practice or until age of 25, whichever is the longer.
- **Personnel and associate records** are maintained and kept up to date whilst the individual works at the practice as an employee or self-employed contractor. Following their departure from the practice their records are retained for six years from the date of leaving the practice. Records relating to workplace accidents or injuries are retained indefinitely. Records for associates are kept for up to eight years.
- **Financial records** are retained for at least six years.
- **Business records**, including contracts with suppliers, are retained for at least six years.

Secure storage

All members of the team must protect information held by the practice and store it securely. Information is only accessed on a need-to-know basis: where it is necessary to carry out required tasks; in the delivery of care to patients; or upon the direct instruction of a senior person within the practice.

For records held electronically, access is password protected and restricted to those who, as part of their work duties, require the information. Electronic records are regularly backed-up by Beverley Mitchelson and the backups are stored off-site in a physically secure location.

Non-electronic (paper) records are stored in a location that is not accessible to patients, visitors to the practice or other members of the public. To ensure that patient record cards, financial information and personnel records are stored securely they must be kept in lockable cabinets at the end of each working day and the keys retained by Beverley Mitchelson.

We store your personal information securely on our practice computer system and in your personal file, which is kept locked in a filing cabinet in the reception office. Your information cannot be accessed by those who do not work at the practice. Only authorised team members have access to your information (on a need-to-know basis). They understand their legal responsibility to maintain confidentiality and follow practice procedures to ensure this.

We take precautions to ensure security of the practice premises, the practice filing systems and computers.

We use high-quality specialist dental software to record and use your personal information safely and effectively. Our computer system has a secure audit trail and we back-up information routinely.

We keep your records for 10 years after the date of your last visit to the Practice or until you reach the age of 25 years, whichever is the longer.

Financial information and personnel records are stored securely in a locked filing cabinet in the practice managers office which is kept locked when unoccupied.

Archiving records

Where records need to be retained but are no longer required on a day-to-day basis, they are archived and stored securely. Records will be stored in a way that ensures easy identification and retrieval. The final decision on archiving information is taken by Beverley Mitchelson.

Electronic records that need to be retained but are not required on a day-to-day basis are, in the first instance, archived within the IT system. Where electronic storage space is at or near capacity, archived electronic data will be copied onto a suitable electronic format with copies stored securely at the practice premises and off-site.

The practice has systems for reviewing archived information that is no longer needed. Personnel information is reviewed annually at the end of March. Patient records are reviewed annually at the end of October. A reminder is in the digital appointment diary.

Secure disposal of old records

Records that are no longer required are disposed of securely by shredding, pulping or incineration. The services of a professional contractor will be used where necessary; a certificate of confidential destruction is obtained and retained by the practice as evidence of DPA compliance.

Patient study models are disposed of as soon as they are no longer required, and at the latest at the same time as the records associated with the patient are disposed of. Study models are removed from the practice using the gypsum waste containers which are provided by SRCL for safe confidential disposal.

Records held electronically and backups of electronic information are disposed of using the secure deletion option on the practice computer system.

The final decision on disposing of records will be taken by Beverley Mitchelson.

Date: 26.04.2018

Review date: 26.04.2018