Beaconsfield Dental Practice

Data Protection Policy

Beaconsfield Dental Practice complies with the Data Protection Act 1998 and general Data protection regulation (GDPR 2018) this policy describes our procedures for ensuring that personal data about patients is processed fairly and lawfully.

Confidentiality

see our confidentiality policy

• All staff employment contracts contain a confidentiality clause.

• Access to personal data is on a "need to know" basis only. Access to information is monitored and breaches of security will be dealt with swiftly by the practice manager.

• We have procedures in place to ensure that personal data is regularly reviewed, updated and deleted in a confidential manner when no longer required.

What personal data do we hold?

In order to provide you with a high standard of dental care and attention, we need to hold personal information about you. This personal data comprises:

1. Your past and present medical and dental condition.
2. Personal details such as your age, NHS number, address, telephone number and the name and address of your medical practitioner.
3. Radiographs, clinical photographs and study models.
4. Information about the treatment that we have provided or propose to provide and it's cost.
5. Notes of conversations/incidents that might occur for which a record needs to be kept.
6. Records of consent to treatment.
7. Any correspondence relating to you with other healthcare professionals, i.e. hospital

Why do we hold information about you?

We need to keep comprehensive and accurate personal data about our patients in order to provide them with safe and appropriate dental care. We also need to process personal data about patients in order to provide care under NHS arrangements and to ensure the proper management and administration of the NHS.

How do we process the data?

We will process personal data that we hold about you in the following ways:

1. Retaining information

We will retain your detail records whilst you are a practice patient, and after you cease to be a patient, for at least 11 years or, for children, until the age of 25, whichever is the longest.

2. Security of information

Personal data about you is held on the practice computer system and in our manual filing system. The information is not accessible to the public and only authorised members of staff have access to it. Our computer system is password protected, has secure audit trails and we take backups regularly. Our processes are audited regularly to ensure compliance with this policy.

3. Disclosure of information

In order to provide proper and safe dental care, we may need to disclose personal information about you to:

- Your general medical practitioner
- The hospital or community services
- Other health professionals caring for you
- NHS payment authorities
- Inland Revenue
- The Benefits Agency, if you are claiming exemption or remission from NHS charges
- Private dental schemes of which you are a member

Disclosure will take place on a 'need to know' basis so that only those individuals/organisations who need to know in order to provide care to you and for the proper administration of the Government will be given the information. Only that information that the recipient needs to know will be disclosed. In very limited circumstances, or when required by law or a court order, personal data may have to be disclosed to a third party not connected to your health care. In all other situations, disclosure will only occur when we have your specific consent. Where possible, you will be informed of these requests for disclosure.

Physical security measures

• Personal data is only taken away from the practice premises in exceptional circumstances and when authorised by the practice manager. If personal data is taken from the premises it must never be left unattended in a car or in a public place.

• Records are kept in a lockable fireproof cabinet, which is not easily accessible by patients and visitors to the practice.
• Efforts have been made to secure the practice against theft, for example, the use of lockable windows and doors.
• The practice has in place a business continuity plan in case of a disaster. This includes procedures set out for protecting and restoring personal data.

Information held on computer
• Appropriate software controls are used to protect computerised records, for example the use of passwords and encryption. Passwords are only known to those who require access to the information, are changed on a regular basis and are not written down or kept near or on the computer for others to see
• Daily back-ups of computerised data are automatically generated by the server computer which is linked to Carestream Dental
• Staff using practice computers will undertake computer training to avoid unintentional deletion or corruption of information
• Dental computer systems all have a full audit trail facility preventing the erasure or overwriting of data. The system records details of any amendments made to data, who made them and when
• Precautions are taken to avoid loss of data through the introduction of computer viruses

4. Access

You have the right of access to the data that we hold about you and to receive a copy. Access may be obtained by making a request in writing. You will be required to pay a fee of £25.00 for access to computer records or £25.00 for access to manual records (including radiographs). We may require evidence of your identity before being able to comply with the request. We will provide a copy of the record, and an explanation of the record if required, within 40 days of the request and payment of the fee.