

Blyth family Dental Practice

Data protection privacy notice for patients

In providing your dental care and treatment, we will ask for information about you and your health. Occasionally, we may receive information from other providers who have been involved in providing your care. This privacy notice describes the type of personal information we hold, why we hold it and what we do with it.

Information that we collect

We may collect the following information about you:

- Personal details such as your name, date of birth, national insurance number, NHS number, address, telephone number and email address
- Information about your dental and general health, including
 - Clinical records made by dentists and other dental professionals involved with your care and treatment
 - X-rays, clinical photographs, digital scans of your mouth and teeth, and study models
 - Medical and dental histories
 - Treatment plans and consent
 - Notes of conversations with you about your care
 - Dates of your appointments
 - Details of any complaints you have made and how these complaints were dealt with
 - Correspondence with other health professionals or institutions
- Details of the fees we have charged, the amounts you have paid and some payment details

Damien Hall is responsible for keeping secure the information about you that we hold.

Our data protection officer, Beverley Mitchelson, ensures that the practice complies with data protection requirements to ensure that we collect, use, store and dispose of your information responsibly.

Those at the practice who have access to your information include dentists, practice manager, hygiene therapist and other dental professionals involved with your care and treatment, and the reception staff responsible for the management and administration of the practice.

How we use your information

To provide you with the dental care and treatment that you need, we require up-to-date and accurate information about you.

We will share your information with the NHS in connection with your dental treatment.

We will seek your preference for how we contact you about your dental care. Our usual methods are telephone, email or letter.

If we wish to use your information for dental research or dental education, we will discuss this with you and seek your consent. Depending on the purpose and if possible, we will anonymise your information. If this is not possible we will inform you and discuss your options.

We may use your contact details to inform you of products and services available at our Practice.

Sharing information

Your information is normally used only by those working at the practice but there may be instances where we need to share it – for example, with:

- Your doctor
- The hospital or community dental services or other health professionals caring for you
- NHS payment authorities

- The Department for Work and Pensions and its agencies, where you are claiming exemption or remission from NHS charges
- Private dental schemes of which you are a member.

We will only disclose your information on a need-to-know basis and will limit any information that we share to the minimum necessary.

In certain circumstances or if required by law, we may need to disclose your information to a third party not connected with your health care, including HMRC or other law enforcement or government agencies.

Keeping your information safe

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.

Access to your information and other rights

You have a right to access the information that we hold about you and to receive a copy. You should submit your request to the practice in writing or by email. We do not usually charge you for copies of your information; if we pass on a charge, we will explain the reasons.

You can also request us to

- Correct any information that you believe is inaccurate or incomplete. If we have disclosed that information to a third party, we will let them know about the change
- Erase information we hold although you should be aware that, for legal reasons, we may be unable to erase certain information (for example, information about your dental treatment)
- Stop using your information – for example, sending you reminders for appointments or information about our service
- Supply your information electronically to another dentist.

If you do not agree

If you do not wish us to use your personal information as described, you should discuss the matter with your dentist. If you object to the way that we collect and use your information, we may not be able to continue to provide your dental care.

If you have any concerns about how we use your information and you do not feel able to discuss it with your dentist or anyone at the practice, you should contact The Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF (0303 123 1113 or 01625 545745).

Date: 26.04.2018

Review date: 26.04.2019

Blyth Family Dental Practice Data security policy

This dental practice is committed to ensuring the security of personal data held by the practice. This policy is issued to all staff with access to personal data at the practice and will be given to new staff during their induction. If any member of the team has concerns about the security of personal data within the practice they should contact Beverley Mitchelson.

All members of the team must comply with this policy.

Confidentiality

- All employment contracts and contracts for services contain a confidentiality clause, which includes a commitment to comply with the practice confidentiality policy
- 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 Beverley Mitchelson.
- We have procedures in place to ensure that personal data is regularly reviewed, updated and, when no longer required, deleted in a confidential manner. For example, we keep patient records for at least 10 years or until the patient is aged 25 – whichever is the longer.

Physical security measures

- Personal data is only removed from the practice premises in exceptional circumstances and when authorised by Beverley Mitchelson. 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 by, for example, the use of intruder alarms, lockable windows and doors
- The practice has in place a business continuity plan in case of a disaster. This includes procedures 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 and weekly back-ups of computerised data are taken and stored in a fireproof container, off-site. Back-ups are also tested at prescribed intervals to ensure that the information being stored is usable should it be needed
- Staff using practice computers undertake computer training to avoid unintentional deletion or corruption of information
- Dental computer systems 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.

Loss of patient information

- Any loss, damage to or unauthorised disclosure of patient information must be reported immediately to Beverley Mitchelson immediately.

Date: 26.04.2018
Review date: 26.04.2019

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

Blyth Family Dental Practice

Access to information held by the practice

We may be asked to disclose information, documents or records held by the practice. Requests for personal information are made under data protection legislation and under freedom of information legislation for information about the NHS services provided by the practice.

Requests for personal information or for information about the practice that is not included in the practice information leaflet should be passed to Beverley Mitchelson.

This policy describes who can request information and how and the practice procedures for managing these requests.

Requests for personal information

Personal information is any information that allows an individual to be identified. This includes information where the individual is not named but a cross-reference to other information held by the practice would allow identification.

Data protection legislation allows individuals to request access to their personal information. Those eligible to request access include:

- A person aged 16 years or older
- The parents or guardians of a child under the age of 16 years and in connection with the health and welfare needs of the child
- A child under the age of 16 years who has the capacity to understand the information held by the practice. Children aged 11 years and under are deemed too young
- A third party, such as a solicitor, who has the written consent of individual concerned – checks should be undertaken to ensure that the consent is genuine – for example, by checking the patient's signature or contacting the patient directly to confirm that they have given consent for the information to be disclosed.

If a request concerns information about a deceased person, those eligible to request access include:

- The administrator or executor of the deceased person's estate
- A person who has a legal claim arising from the person's death – the next of kin, for example. The person should explain why the information requested is relevant to their claim.

If the information requested includes information about third parties, it can be disclosed if the third party gives consent or is a health professional involved in the care of the patient.

The request

The request must be made in writing and describe the type of information required with dates, if possible, and include sufficient information to ensure correct identification (name, address, date of birth, for example). You must check that the person asking for information has the right to do so and, if necessary, ask for proof of identity.

We will provide the requested information within one month of receiving the request or confirming the individual's identity.

The information

We will usually provide the information requested in electronic form using secure means, unless the individual asks for the information in paper format or otherwise agreed. The individual may also come to the practice to view the original version under supervision and on practice premises.

We will provide the information in a way that can be understood by the individual making the requests and may need to provide an explanation to accompany dental clinical notes.

Unfounded or excessive requests

Where requests are manifestly unfounded or excessive (particularly if they are repetitive), we can:

- Charge a reasonable fee taking into account the administrative costs of providing the information; or
- Refuse to respond.

If we refuse to respond to a request, we will explain the reasons and informing the individual of their right to complain to the Information Commissioner's Office and to a judicial remedy.

Requests for information about the practice

Freedom of information legislation allows anyone to ask for information about the provision of NHS services. The available information is described fully in the practice guide to information available under FOIA and the model publication scheme. If the requested information is part of a larger document, we will disclose only the relevant part.

A freedom of information request cannot include clinical records or financial records.

The request

The request must be made in writing and should describe the type of information that they want and with dates, if possible. The individual making the request does not have to give a reason.

The charges for information provided under a freedom of information request are included in the practice guide and the model publication scheme

We will provide Information within 20 working days of receiving the request or confirmation of identity or, if applicable, from the receipt of the fee.

It may be possible to extend this timescale if we need more information about the request or are taking legal advice on whether an exemption applies. We must inform the person making the request if we need to extend the 20-working-day deadline.

The information

Most of the information covered by a freedom of information request is available in the practice information leaflet or on the practice website. Requests for other information should be referred to Beverley Mitchelson. If we do not hold the information requested, we will inform the individual within the 20-working-day time limit.

We will provide information in a way that is convenient for the person who requested it, which may be in writing, by allowing the applicant to read it on the premises, or, if the information is held electronically, in a useable electronic format.

We are not required to respond to

- Vexatious requests for information, for example, requests that are designed to cause inconvenience, harassment or expense.
- Repeated requests for the same or similar information (unless the information changes regularly, for example performance or activity information)

In either situation, you should seek advice from Beverley Mitchelson.

Date: 26.04.2018

Review date: 26.04.2019