DATA PROTECTION POLICY and CODE OF PRACTICE

Why we have this Policy

This practice collects and stores information and is therefore legally obliged to ensure that all personal data is protected. The practice is registered under the Data Protection Laws with the Information Commissioner and there are heavy penalties for infringement of the Data Protection Act 2018 and UK GDPR (2021)

It is important therefore that every team member understands how and why we use such data and how it must be stored and handled securely. We only hold information that is relevant and only for as long as it is needed.

Our data protection code of practice provides the required procedures to ensure that we comply with the Data Protection Act 2018 and UK GDPR 2021. It is a condition of engagement that everyone at the practice complies with the code of practice.

Introduction

Please read the following policy carefully. You should ask Sonam Soni (Data Controller named in the GDPR. who is in charge of the correct operation of this policy if there is anything about which you are unsure.

Team members must

At all times, comply with the principles of the Data Protection Act 2018 and UK GDPR (2021):

Never name, or discuss identifiable information, about a patient/ Staff member outside the practice, including with friends or relatives of the patient/Staff member.

Never post pictures or information which could identify a patient/Staff member on any social media site.

- Store patient records securely and confidentially where it is not possible for other patients or individuals to read them or any other visiting providers e.g. out of hours cleaners
- Store all staff records securely and confidentially.
- Ensure that information about patients is never left unattended (e.g. on a screen at the reception desk or paper records left in surgery or at reception) particularly also screens associated with digital radiography in public or semi – public unattended areas
- Store paper records in lockable filing cabinets. WHICH ARE LOCKED WHEN UNATTENDED, or within a secure and locked room only available to staff
- Not disclose to any other person or agency (such as a school or college) information as to whether a patient has attended for an appointment on a particular day or even is a patient of this practice. It might be suggested that the patient is asked to obtain the dentist's signature on his or her appointment card to signify attendance if proof is required.

Not provide information about a patient's appointment record to a patient's employer

- Ensure that when talking to a patient on the telephone or in person in a public area, other people cannot overhear sensitive information.
- Ensure that discussions about patients do not take place in the practice's public areas

• Ensure that messages about a patient's care are not be left with third parties or left on answering machines. A message to call the practice is all that can be left
• Ensure that password-protected computer records are backed-up every day, with back-ups stored away from the practice
Ensure that the computer screen is NOT VISIBLE by patients or members of the public when standing at the reception desk or public area.
• Ensure the appointment book and day list are not visible to patients or anyone not involved in patient care

Never disclose patient information to a third party without express consent of the patient, including confirming that someone is a patient at the practice or that they have an appointment. This includes disclosure of appointment books, day sheets or computer screens to police officers or Inland Revenue officials, unless on the specific instructions of the dentist

- Data must not be removed from the practice and if it is required to convey data to another person (e.g. for referral purposes) this is always made by means of a secured or encrypted method.
- Post all written communications, including recalls or reminders, in an envelope
- If called upon to demonstrate the practice's administrative/computer systems, don't allow actual patient information to be used.
• Ensure that there is a named person ready to receive any transmitted information e.g. faxes regarding patient referral to third parties safe haven.

What is 'personal information?'
In a dental context personal information held by a dentist about a patient includes:

• The patient's name or even their 'nickname' or preferred name as written on a Record, current and previous addresses, bank account/credit card details, telephone number/e-mail address and other means of personal identification such as his or her physical description
• Information that the individual is or has been a patient of the practice or attended, cancelled or failed to attend an appointment on a certain day
• Information concerning the patient's physical, mental or oral health or condition or protected characteristics
• Information about the treatment that is planned, is being undertaken or has been provided
• Information about family members and personal circumstances supplied by the patient or others
• The amount that was paid for treatment, the amount owing, or the fact that the patient is a debtor to the practice.

Personal information is also held in this practice for all staff members and this will include
• name, current and previous addresses
• Bank account/credit card details and financial details
• Telephone number/email address
• Physical, mental or oral health or condition including vaccination log
• EDBS disclosure numbers. The EDBS Disclosure is strictly confidential
• Training records
• Family members and personal circumstances supplied including 'nick names'

Disciplinary Action
If, after investigation, a team member is found to have breached Data Protection, he or she shall be liable to summary dismissal in accordance with our practice disciplinary policy.

Access to records

Patients have the right of access to their health records held on paper or on computer that we hold about them and to receive a copy, or they may authorise a third party, such as a lawyer, to do so on their behalf. Parents may access their child's records if this is in the child's best interests and not contrary to a competent child's wishes. Formal applications for access must be in writing to Sonam Soni and accompanied by the appropriate fee (If applicable).

A request from a patient to see records or for a copy must be referred to the patient's dentist. The patient should be given the opportunity of coming into the practice to discuss the records and will then be given a photocopy. Care should be taken to ensure that the individual seeking access is the patient in question and where necessary the practice will seek information from the patient to confirm identity.

Access may be obtained by the patient making a request in writing. There is normally no fee payable for this. We will provide a copy of the record as soon as possible and within 30 days at the latest.

Subject Access Request

GDPR grants people whose personal data is being held (known as Data subjects) by your Practice the right to access such personal data. This is referred to as a subject access request. Such requests by data subjects for the information held about them must be responded to promptly (within a month).

Practices need to update how they manage requests for information. In most cases, practices may not make a charge for providing this unless it can be shown that there is a material cost e.g. copying of radiographs. A practice may refuse or charge if a request is considered manifestly unfounded or excessive. If you refuse a request, you must explain without delay that the patient has a right to complain to the supervisory authority such as the ICO.

IMPORTANT

Because patients have the right of access to their records, it is essential that information is properly recorded. Records must be:

- Contemporaneous and dated
- Accurate and comprehensive
- Signed by the dentist
- Strictly necessary for the purpose
- Not derogatory
- Unproblematic if such a disclosure to the patient needs to be made

If a patient does not agree

If a patient does not wish personal data that we hold about them to be disclosed, updated or used in the way that is described in this Code of Practice, they must be allowed to discuss the matter with their dentist; however this may affect our ability to provide them with dental care and they must be made aware of this.
The patient **does not** have a right to anonymity for medical records.

If your employment at this practice has ended

You are reminded that all personal data processed at the practice must by law remain confidential after your employment has terminated. It is an offence under section 55(1) of the Data Protection Act 1998, knowingly or recklessly to obtain, disclose or procure information without the consent of the practice data controller. If the practice suspects that you have committed such an offence, it will contact the Office of the Information Commissioner and you may be prosecuted.

The rights for individuals to have personal data erased

- The UK GDPR introduces a right for individuals to have personal data erased.
- The right to erasure is also known as 'the right to be forgotten'.
- The right is not absolute and only applies in certain circumstances.
- Individuals can make a request for erasure verbally or in writing.
- You have one month to respond to a request.
- This right is not the only way in which the UK GDPR places an obligation on you to consider whether to delete personal data.

The UK GDPR specifies the right to erasure will not apply to special category data: *"if the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; **for the provision of health or social care**; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional)."*

Link to the ICO guidance on Special Category Data –
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

The UK GDPR defines special category data as:
- *personal data revealing racial or ethnic origin;*
- *personal data revealing political opinions;*
- *personal data revealing religious or philosophical beliefs;*
- *personal data revealing trade union membership;*
- *genetic data;*
- *biometric data (where used for identification purposes);*
- *data concerning health;*
- *data concerning a person's sex life; and*
- *data concerning a person's sexual orientation.*

DATA PROTECTION CODE OF PRACTICE

INFORMATION FOR PATIENTS AND STAFF MEMBERS

We will keep your records secure

This practice complies with the Data Protection Act (1998) and General Data Protection Regulation (GDPR) 2018. This means that we will ensure that your information is processed fairly and lawfully.

What personal information do we hold?

- Your past and current medical and dental condition; personal details such as your age, national insurance number/NHS number, address, telephone number and your general medical practitioner
- Radiographs, clinical photographs and study models
- Information about the treatment that we have provided or proposed and its cost
- Notes of conversations or incidents that might occur for which a record needs to be kept
- Records of consent to treatment
- Any correspondence relating to you with other health care professionals, e.g hospital or community services.
- Employment/Training records
- EDBS Disclosure Numbers

Why do we hold this information?

We need to keep accurate personal data about patients and staff member in order to provide you with safe and appropriate dental care and services. We also need to process personal data about you if we are providing care under NHS arrangements and to ensure the proper management and administration of the NHS.

Retaining information

We are required to retain your dental records, X rays and study models while you are a patient or staff member of this practice and after you cease to be a patient/employee, for at least eleven years, or for children until age 25, whichever is the longer. For staff members we need to keep records for up to 5 years.

Security

Your information is held in the practice's computer system and/or in a manual filing system. The information is only accessible to authorised team members and Care Quality Commission Inspectors. Our computer system has been secured with audit trails and information is regularly backed up to ensure it is not lost.

We may need to disclose your information

In order to provide proper and safe dental care to:

- Your general medical practitioner
- The hospital or community dental services
- Other health professionals caring for you
- NHS payment authorities
- The Inland Revenue
- The Benefits Agency, where 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 Government (whose personnel are covered by strict confidentiality rules) 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 with your health care. In all other situations, disclosure that is not covered by this Code of Practice will only occur when we have your specific consent. Where possible you will be informed of these requests for disclosure.