Data Protection Policy

Introduction

Ivybridge Dental Centre needs to collect and use certain types of information about the people that use and work in the practice, for it to conduct its work and fulfil the requirements of the NHS contract. Any personal information must be collected and dealt with appropriately, whether on paper, in a computer or recorded on other material.

The General Data Protection Regulation 2018 (GDPR) makes organisations more accountable in the way that they collect, use, store and dispose of personal information and gives individuals more control over information about them that they pass onto others.

Ivybridge Dental Centre aims to fully comply with GDPR and all other Data Protection Regulations. This policy describes our procedures for ensuring that personal information about patients and staff is processed in accordance with the six key principles of the General Data Protection Regulations (GDPR).

What personal data do we hold?

We aim to hold the minimum amount of personal data on patients and staff to meet our requirements, to ensure it is kept up to date and to dispose of it appropriately.

Patients Data

To provide patients with a high standard of dental care and attention, we need to hold personal information about them. This personal data comprises:

- Past and current medical and dental conditions;
- personal details such as age, national insurance number/NHS number, address, telephone number
- general medical practitioner.
- Information about the treatment that we have provided or propose to provide and its cost
- Any correspondence relating to patients with other health care professionals, for example in the hospital or community services.

Employee Data

- Personal details such as name, date of birth, national insurance number, passport details or information about their right to live and work in the UK, address, telephone number and email address.
- Bank details
- Relevant information about their health, including immunisations against hepatitis B and other blood-borne viruses
- The results of criminal-record checks obtained from the Disclosure and Barring Service

Associate Data

- Personal details such as name, date of birth, national insurance number, passport details or information about their right to live and work in the UK, address, telephone number and email address.
- Bank details
- Relevant information about their health, including immunisations against hepatitis B and other blood-borne viruses
- The results of criminal-record checks obtained from the Disclosure and Barring Service

Why do we hold this data?

We need to keep comprehensive and accurate personal data about our patients to fulfil our contract with them to provide safe and appropriate dental care including providing care under NHS arrangements.

We need to keep comprehensive and accurate personal data about our employees and associates to comply with legal obligations required by HMRC, the GDC, NHS, CQC and other regulators or government bodies and to meet our contractual obligations to them as employees or associates.

Where do we hold the data and how do we process it?

We hold patient data in our dental software and this is used to process claims for NHS treatment and to record and plan dental treatment. We hold patient contact details in the same system so that we can send emails, texts and/or letters to patients regarding their appointments and treatment plans. Patients are asked how they prefer to be communicated with.

We hold personal staff data in their personnel files and payroll software. We process staff bank details and information regarding their tax codes, so that we can pay them and ensure we pay their TAX, NI and pension contributions. We process staff contact details so that we can keep them informed of changes to work schedules.

Security of information

Personal data is held in the practice's computer system and/or in a manual filing system. The information is not accessible to the public and only authorised members of staff have access to it. Our computer system has secure audit trails and we back up information routinely.

Sharing of information

To provide proper and safe dental care, we may need to disclose personal information about patients to:

- A patient's general medical practitioner.
- Hospital or community dental services.
- Other Health professionals caring for a patient
- NHS payment authorities.
- HM Revenue and Customs
- The Department of Work and Pensions and its agencies where you are claiming exemption or remission from NHS charges.
- Private dental schemes if a patient is a member.

Disclosure will take place on a 'need to know' basis, so that only those individuals/organisations who need to know to provide care to a patient and for the proper administration of 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 with your health care. In all other situations, disclosure will only occur when we have your specific consent.

Right to be informed including privacy notices

We provide privacy notices to patients, employees and associates and review them annually. These explain what data we collect and why, how it is stored and processed and how it is disposed of.

Right of access

Patients have the right of access to the personal data that we hold about them and to receive a copy. Access may be obtained by making a request in writing. We will require evidence of identity before being able to comply with the request. We will provide a copy of the record within 40 days of the request and an explanation of your record should you require it.

Right to rectification and data quality

We ensure that the personal data we hold remains accurate and up to date:
Patients and staff are regularly reminded to notify the Practice if any of their relevant personal details change.
Requests from individuals to have their personal data corrected will be met within 1 calendar month.

Right to erasure including retention and disposal

We will retain dental records whilst patients are considered a patient of the practice and after they cease to be a patient for at least eleven years or, for children, until age 25, whichever is the longer. Patients have the right to be forgotten and can request the erasure of personal data, when they leave the Practice, unless it must be kept for legal reasons.

We will retain staff employment records for 6 years after the end of their employment.

Paper records containing personal information that is no longer required will be shredded and digital records deleted.

Right of data portability
Patients can ask us to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability. Requests will be handled by the Practice Data Protection Officer within 1 month and where it is not possible to transfer electronically a p

Right to object
Patients and staff are informed of their right to object to the way we use their personal data in our Privacy Notices.

Governance and Accountability

Data Protection Lead
The Practice lead on Data Protection is Peter Reville. Their task is to:
- inform and advise the dental team of its obligations to comply with the GDPR and other data protection laws
- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities and advise on data protection impact assessments
- train staff, conduct internal audits and be the first point of contact for individuals whose data is processed.

Data processor contracts
Currently the Practice does share patient data with Devon Dental Laboratory and IW Dental Laboratory. We have data sharing agreements in place with them.

Data Protection Impact Assessments (DPIA)
The Practice will carry out a DPIA when introducing new technologies or if processing is likely to result in a high risk to the rights and freedoms of individuals.

International transfers
The Practice will not transfer personal data outside the EU.

Breach notification
Should the Practice become aware of a personal data breach (i.e. the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data) the Practice Owners will assess if it is likely to result in a risk to the rights and freedoms of individuals. If it is assessed that it will, then the ICO must be informed within 72 hours.

If the breach is likely to result in a high risk to the rights and freedoms of the individuals then we will notify those concerned directly and without undue delay.

Annual Review
This policy will be reviewed annually and issued to all employees and associates who implement the policy.

Date: 2.6.21