

Hilltop Dental Practice – GDPR - Principals

The GDPR, or General Data Protection Regulation, is a piece of European legislation which replaced the Data Protection Act (DPA) 1998 on 25 May 2018. The New Data Protection Act 2018 also came into force at the same time. The purpose of the new DPA is to apply the GDPR in the UK. The underlying data protection principles have not changed significantly from those of the DPA – but there is the new principle of ‘accountability’. The GDPR also requires organisations to adopt the philosophy of ‘data protection by design and default’. This means that the organisation must be able to demonstrate compliance with the data protection principles. The principles are the backbone of the regulation.

Data Protection Officer is The Practice Owner

The individual responsible for ensuring that our practice complies with data protection laws. They act as a liaison between the business, data subjects, and regulatory authorities. Essentially, the Data Protection Officer ensures data privacy and security within Hilltop Dental Practice.

Staff Training:

Are staff are trained to ensure that they follow GDPR principles.

What personal data do we hold:

***Patients**

Personal details, family members, treatment details, medical history, financial details regarding payments and bank account details for those paying by direct debit.

***Staff**

Personal details, some medical information if required for their safety at work, employment history, NI number, bank account details, salary, results of DBS checks, references.

All information is kept confidentially within the practice or with trusted partners. Only the information that is necessary to provide treatment, manage appointments and manage dental plans is gathered in order to enable the practice to provide care and treatment to patients.

For staff, personal information, previous employment details, DBS checks and references are required to ensure that staff are suitable for their position within the practice and can work safely.

Information is gathered directly from staff and patients, references and DBS checks are gathered after obtaining consent.

We may share information with other partners for treatment referrals or for training purposes to receive personalised certification.

Legal Grounds for processing data:

1. Consent: We need to obtain explicit, informed consent from patients to process their personal data.
2. Contract: We have a duty of care to our patients to provide the required treatment to maintain their dental health and this requires the practice to obtain essential information like patient identification and contact details for appointment scheduling, and billing.
3. Legal Obligation: Dental practices have legal obligations to comply with regulations and laws related to patient data, including data protection laws and standards of care. This may involve keeping records, reporting certain events, or complying with data breach notification requirements.
4. Vital Interests: In certain circumstances, processing patient data may be necessary to protect their vital interests, such as in an emergency where an individual is incapacitated and unable to provide consent for treatment.
5. Public Task: The practice provides some services under an NHS healthcare system requiring us to process patient data to fulfil our public duty.
6. Legitimate Interests: The practice also processes data based on legitimate interests. This is balanced against the data subject's rights and freedoms. This could include using patient data to improve our services for example requesting feedback, providing information for example changes within the practice that affect patient care or for internal administrative purposes for example auditing.

The information that we hold is kept for the minimum amount of time required and then disposed of appropriately and securely.

We have policies in place to support patient consent, confidentiality, data security, access to information, internet use. Our policies include information about identifying breaches and how to report data breaches.

We have evidence in place to demonstrate our partners (third parties) follow GDPR compliance and keep information safe.

We have a privacy notice on our web site, in the waiting room and available for patients if they request a copy.

We respect individuals rights:

- To be informed
- To have access to their information
- To rectify any mis information
- To restrict processing
- To erase information held (within legal remits)

- To data portability
- To object