Data Protection Policy

The Data Protection Acts (1984 and 1998) were introduced to safeguard the holding and processing of personal data in an increasingly computer-driven age. The 1984 Act applied wholly to electronic data, whilst the 1998 Act extends controls to paper records as well.

For dentists, there are the additional requirements of the General Dental Council on patient confidentiality, as well as the Access to Health Records Act 1971 to take into consideration. The GDC's requirements are professional, rather than legal, whilst the 1971 Act has implications for all health professionals: its requirements are not, largely, superseded by the Data Protection Act. Additionally, European Directives applying to Data Protection are also now in place and apply to all forms of data.

The Practice's data protection policy is compliant with GDPR.

Whilst dental practices will already be conversant with the requirements and significance of the Data Protection Act 1998, this new Legislation introduces some changes that data controllers need to adopt.

Legal requirements

The following requirements apply to Peasholm dental practice:

- As we have a practice computer system which records any personal data (see below), we are registered with the Information Commissioner (website references at the end of this section), and maintain our registration on an annual basis.
- We have a data protection policy and ensure that everyone complies with it and the requirements of the Acts.
- We have a record keeping policy, and access to information held by the practice policy in place for responding to requests for data access by subjects (such as a current or former staff, patients or their representatives).

Professionally, the GDC requires we maintain strict confidentiality in relation to all dealings with patients, including, but not limited to, their personal data.
The principal dentists are currently registered directly with the Information Commissioner's Office. Certification can be located on our intranet, on our website and in our waiting room.

About data protection

There are eight data protection principles with which all data users (including us as dentists) must comply. Personal data must be:

- Processed fairly and lawfully.
- Processed only for specified purposes and in an appropriate way.
- Relevant and sufficient for the purpose.
- Accurate and up to date.
- Kept only for as long as necessary.
- Processed in accordance with individuals' rights.
- Kept secure.
- Transferred to countries outside Europe only if the receiving country has equivalent controls.

Definitions

Data: information which is stored in a computer or a structured (e.g. alphabetical) paper file.

Personal data: essentially factual or biographical data about a living individual from which they can be identified (Note: individuals, not firms or companies; living, not deceased). It can be factual (name address, phone number, email address) or an opinion (e.g. diagnosis).

Processing: any action involving the data i.e. obtaining, storing, sorting, updating or deleting it.

Data Controller: People or organisations which store or use data (e.g. dentists). They decide what data is needed and how it is used. They have the legal responsibility for registering and having policies.

Data processor: Organisations who process data for data controllers (e.g. Denplan, Dental Practice Board). They do not own the data nor decide how it is processed. They also have to follow the Act and ensure data is handled properly.

Data subjects: people the information is about. They have rights in relation to their data.

Sensitive data: personal data falling into specific categories such as health, race, ethnicity, politics, religion, sexual life, criminal convictions. Processing this

data requires the subject's consent. A dental patient is considered to have consented by agreeing to be examined or treated.

What is covered?

Computer data which relates to individuals.
Paper files (e.g. clinical notes) which are organised by identifiers such as name, address etc.(Largely discontinued now)
Emails.
Recorded telephone calls, answering machine tapes.
CCTV footage
Notepads, such as telephone jotters which can be used to identify people.

A data protection policy

This is required for each registered organisation.

Freedom of Information Act

The Freedom of Information Act 2000 (FOIA) and the Freedom of Information (Scotland) Act 2002 (FOISA) give individuals a general right of access to all types of recorded information held by public authorities in the United Kingdom. The Acts places a number of obligations on public authorities and the public has the general right to access information held by public authorities. Dentists providing general dental services (GDS) or Personal Dental Services (PDS) are listed as public authorities.

FOIA and FOISA mean that: dentists will have the right to ask for information held by a Primary Care Organisation (PCO, that is a Primary Care Trust or Health Board); and that members of the public will be able to request information held by GDS and PDS practices.

These Acts, require all organisations to have a "publication scheme" which sets out a list of all the information it holds and which it is prepared to supply to any interested person. Originally, it was believed that this included financial data, but following negotiations between the BDA and the Information Commissioner, this requirement has now been omitted.

However, it remains a legal requirement for all dental practices to have such a scheme in place (from October 2003 in England and Wales, and from January 2005 in Scotland).
The Act confers two statutory rights on applicants:

- To be told whether or not the public authority holds the information requested; and, if so,

- To have that information communicated to them (subject to a schedule of allowed exclusions

See the relevant sections (FOI Acts) of the Information Commissioners' websites given below.

Every public authority must routinely publish information, respond to requests for information and adopt a publication scheme. The sort of information that NHS general dental practices must routinely publish will mostly be covered in their patient information leaflet – make sure this is freely available.

A publication scheme is a document that should set out for the public how the public authority intends to publish the different classes of information it holds and whether there is a charge for the information. NHS general dental practices must have their own publication scheme.

Confidentiality

As noted previously, confidentiality is a professional requirement imposed and regulated by the General Dental Council (GDC). Only in exceptional circumstances, (e.g. where a major crime is being investigated, or to comply with specific laws such as Road Traffic Acts or terrorism) should any information about patients be divulged without their specific prior consent. Disclosure to a specialist or other health professional directly concerned in a patient's care is also accepted, provided the patient is aware of the referral.

The GDC takes very seriously any allegation of breach of confidentiality relating to a patient. We endeavour to do everything possible to avoid such breach. please see accidental disclosure of data.

Access to Health Records Act 1971

This Act relates principally to the rights of a patient to access their own health records. This right is generally upheld legally, and only in exceptional circumstances (e.g. where such access could be shown to have a potentially serious effect on the patient's mental or physical health, or where the records include references to third parties whose confidentiality might be infringed) should such a legitimate request be denied.
We always endeavour to follow the guidance of GDPR and provide subjects with the data requested, where the request is reasonable. We do not charge for reasonable requests, and provide these to the subject within 30 days. We don on some occasion charge a small administration fee.

Data Protection and Self Employed Associates

Although Associates are mostly self-employed, their circumstances will dictate whether they are a Data Owner, or a Data Processor. In the former case, they need to register individually with the Information Commissioner at an annual renewable cost.

If, on the other hand the control of data in the practice is in the hands of the practice owner/s and the associate is only processing it under direction (this should be included in an Associate Agreement, with requirements to abide by the practice Data Protection, confidentiality, security, and information governance policies), then they may not be considered to "own" the data and may not need separate registration. This should be considered by the practice as a whole.

In some circumstances, Primary Care Trusts or Local Health Boards may consider that an associate with an individual NHS contract is in any event the "data owner" so far as the NHS is concerned. In this case, ICO registration will be necessary.

Our associates are currently data processors only, due to their current work situation.

Further information and contacts

To register with the Information Commissioner go to
http://www.informationcommissioner.gov.uk