Data Protection Impact Assessment

Data protection impact assessment (DPIA) is a process to help you identify and minimise data protection risks. Such assessments are a means of demonstrating that measures are in place to safeguard patient information. These assessments are legally required if the way in which information is handled has the potential to breach confidentiality. For example, you will need to do a DPIA if you install new patient record software, or a new system for sharing information or making referrals.

1. Identify the need for a DPIA

At BRANDHALL Dental Practice; we are dedicated to processing patient data safely. For further information, please take a look at our 'Privacy Notice' located in reception, or alternatively speak to a member of our team.

It is our aim to reduce any risks of confidentiality or data breaches within the dental practice. Information will only be shared when it is needed to make direct care and treatment easier and faster with consent from the patient or guardian. We will never share any information without the consent to do so. For example, this could include allowing a dentist to see the medication that a GP has prescribed for a patient or allowing a dentist to refer for services such as sedation, treatment under general anaesthetic and Dental Hospital treatments that we cannot offer at our practices.

2. Describe the processing

We will ask patients to provide personal information when joining the practice. The purpose of us processing this data is to provide optimum health care to our patients.

The categories of data we process are:

- Personal data for the purposes of staff and self-employed team member management
- Personal data for the purposes of direct mail/email/text/ reminders (This can be opted out on our Medical History Questionnaire)
- Special category data including health records for the purposes of the delivery of health care
- Special category data including health records and details of criminal record checks for managing employees and contracted team members (For example, DBS checks on employees)

Data we collect from patients and used are:

- Patient name(s)
- Date of birth
- Address
- Contact information
- Medical histories and a list of medications
- NHS proof of exemption if any
- Treatment details

- Appointment history and details

Patient records are kept in line with our record retention policy. All patient records are kept secure and can only be accessed by approved staff, who have individual logins for our dental software. Patient records may include children or other vulnerable groups.

Dental care professionals at the practice accessing information will have a legitimate relationship with the person whose information they are accessing, i.e. they are directly responsible for providing dental care for that person. Individuals generally expect their information to be shared between health care professionals who are responsible for their care. Many shared health records exist across the country; however we do not share any records to third parties without prior consent to do so.

There are no prior concerns over this type of processing and there are currently no security flaws. There are no current issues of public concern. Our current state of technology in the area of data processing is kept secure at all times.

The purpose of processing data is to achieve our aim to reduce any risks of confidentiality or data breaches within the dental practice. The intended effect on patients will be a seamless, high quality service with reminders they can opt out of at any time.

3. Consultation process

As we are an NHS dental practice, any data we may share to 'processors' with patient consent to do so would be to:

- Referral services
- Dental laboratories

Any outsourced departments have a data processing agreement with our practice so comply with the GDPR and patient safety.

4. Assess necessity and proportionality

The primary consideration of Brandhall Dental Care is to improve the quality of dental health and care whilst maintaining the highest levels of confidentiality. All dental care providers are subject to the statutory duty under section 251B of the Health and Social Care Act 2012 to share information about a patient for their direct care. This duty is subject to the common law duty of confidence, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Under GDPR there must be a valid lawful basis to process personal data. For GDPR sharing information is on the basis of public task where "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

There are legal provisions that support the release of data for the purposes of safeguarding children and vulnerable adults. The Children Acts 1989 and 2004 establishes implied powers for local authorities to share information to safeguard children, safeguard and promote the welfare of children within their area who are in need, and to request help from specified authorities including

NHS organisations. The Care Act 2014 sets out a legal framework for how local authorities and other parts of the health and social care system should protect adults at risk of abuse or neglect.

5. Identify and assess risks

Describe the source of risk and nature of potential impact on patients	Likelihood of harm	Severity of harm	Overall risk
There is a risk that patients may miss out on the highest quality of dental care. Their shared health and care record not being available at the point of care, or data may not be accurate.	Possible	Minimal	Low
There is a risk of stress and damage to individuals. Data could be made available to others without permission or knowledge. Information may be shared against individual wishes or may be made available to the wrong persons. Vulnerable and minority groups may not be sufficiently aware of the system and what their data is being used for.	Possible	Minimal	Low
There is a risk to compliance with regulations - GDPR, Equality & Diversity Regulations, Duty of Care, Confidentiality, Health & Social Care Act 2016	Possible	Minimal	Low

6. Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
There is a risk that patients may miss out on the highest quality of dental care.	Ensure all data is available and accurate. Medical history questionnaires to be updated every new course of treatment and	Reduced	Low	Yes

	recorded onto the system.			
There is a risk of stress and damage to individuals.	Privacy Management to manage opt out and other aspects. Training of staff should ensure that the patient is content for them to view their record at point of care. Robust training programme to inform clinicians re use of data.	Accepted	Low	Yes
There is a risk to compliance with regulations	Robust governance developed to review requests for data	Accepted	Low	Yes

7. Sign off and record outcomes

Item	Name / date	Notes
Measures approved by:	Karen Wheller 20.12.18	
Residual risks approved by:	Karen Wheller 20.12.18	
DPO advice provided:	Charlotte South 20.12.18	
Summary of DPO advice: Continue to strive for excellent dental care to all of our patients, as well as complying with the GDPR, IG and all other policies and procedures in place at our practices. Processing can proceed.		
DPO advice accepted by:	Karen Wheller 20.12.18	

This DPIA will be kept under review by:	Karen Wheller	The DPO should also review ongoing compliance with DPIA