Cemaes Bay Dental Practice

Legitimate Interest Assessment

Document ID: 2018_04_028

Document Created By: DJM

Date: 04/2018 Review due: 04/2020

Updated By:	Date:	Next Review Due:

General Data Protection Regulations
Legitimate Interest Assessment
Cemaes Bay Dental Practice

Part A: Identifying a Legitimate Interest		
Question		**Response**
1.	What is the purpose of the processing operation?	In order to safely carry out dental care and treatment of patients and to comply with legislative and legal requirements.
2.	Is the processing necessary to meet one or more specific organisational objectives?	Yes – it is a legal and professional requirement
3.	Is the processing necessary to meet one or more specific objectives of any Third Party?	Yes - to conform to General Dental Council Standards and to maintain high professional standards as defined by expert authorities. - To meet legal and contractual requirements with the NHSBSA, HMRC - To enable administration of patient registration schemes such as Denplan and Lloyd and Whyte -
4.	Does the GDPR, ePrivacy Regulation or other national legislation, specifically identify the processing activity as being legitimate, subject to the completion of a balancing test and positive outcome?	Yes – Article 9(2) of the GDPR and Clause 10(2) of the Data Protection Act 2017 refers to the processing of sensitive personal data.

Part B: The Necessity Test		
Question		**Response**
1.	Why is the processing activity important to the Data Controller?	To maintain current accurate records of patients' health care and treatment and to identify them for administrative purposes
2.	Why the processing activity is important to other parties the data may be disclosed to (if appropriate)?	To ensure the provision of high quality care and treatment to patients as appropriate to their needs; and to ensure the accessibility and accuracy of the records. E.g. dental laboratories and other suppliers, referral practices, clinical data processors (software suppliers) and other expert advisers
3.	Is there another way of achieving the objective?	No

Part C: The Balancing Test		
Question		Response
1.	Would the individual expect the processing to take place?	Yes
2.	Does the process add value to a product or service that the individual uses?	Yes
3.	Is the processing likely to negatively impact the individual's rights?	No
4.	Would there be a prejudice to the Data Controller if processing did not take place?	Yes
5.	Is the processing likely to result in unwarranted harm or distress to the individual?	No
6.	Would there be a prejudice to a Third Party if processing did not happen?	No
7.	Is the processing in the interests of the individual whose personal data it relates to?	Yes
8.	Are the legitimate interests of the individual aligned with the party looking to rely on their legitimate interests for processing?	Yes
9.	What is the connection between the individual and the organisation?	- Existing customer - Lapsed or cancelled customer - Employee or contractor - Business client - Prospective client - Supplier
10.	What is the nature of the data to be processed? Does data of this nature have any special protections under GDPR	- Identification of the individual - Contact details - Current and past health data (Sensitive) - Future clinical care and treatment (Sensitive)
11.	Is there a two-way relationship between the organisation and the individual? How close is that relationship?	- On-going
12.	Would the processing undermine or limit the individual's rights?	No
13.	Has the personal data been obtained directly from the individual?	- Yes – in the case of consenting adults - No – in the case of children below the age of consent and vulnerable adults

14.	Is there an imbalance in who holds the power between the organisation and the individual?	Yes, however the obtaining of valid consent to care and treatment by each individual or an appointed carer, parent or Attorney validates the processing
15.	Is it likely that the individual would expect their information to be used for this purpose?	Yes
16.	Could the processing be considered intrusive or unwarranted? In particular, could it be perceived as such by the individual, or in the context of the relationship?	No. Processing is subject to the requirements of professional confidentiality
17.	Is a fair processing notice supplied to the individual? If so, how? Is it sufficiently clear and up front regarding the purpose of the processing?	A full Privacy Notice is available on websites, and at the premises and its existence is clearly signposted in all means of contact
18.	Can the individual whose data is processed control the processing or object to it easily?	Access to clinical records is available to every patient. Records of patients not under continuing or regular care are archived for legal purposes as required by professional authorities
19.	Can the scope of the processing be modified to reduce or mitigate any underlying privacy risks or harm?	See mitigations in Part D

Part D: Safeguards and Compensating Controls

- Access to records is only available in areas without public access – eg behind reception desks
- Data is kept secure with computer terminals that require passwords which are changed monthly.
- Personal data storage devices or equipment is not to be attached to the practice systems or networks..
- Public WiFi is isolated from practice networking and is only available during normal opening hours of the practice.
- Staff training and confidentiality clauses in contracts ensure all members of the team are knowledgeable about data security
- Premises are secured with high-security locks and alarm system which is maintained.
- Data is backed up in multiple secure locations to ensure it is preserved in the event of catastrophic damage to the practice
- Cloud back-up storage options are GDPR compliant and have additional security in place to minimise the risk of disclosure.
- Non-essential data has an opt-out option – eg electronic messaging for reminders.

E: Outcome of Assessment:

- Data processing within the practice is essential for the provision of high quality clinical care and treatment
- Patients would expect processing and storage as a norm
- Professional and legal safeguards for security and accuracy of data apply and are adopted fully
- Care is taken not to undertake unnecessary or excessive processing
- Data is archived according to authoritative guidance for the purpose of legal accountability

Therefore, I believe the Legitimate Interest threshold is met

(Signed Electronically) David Meacher Date: 10/04/2018