HC Christensen Dental Practice
May 2018

GDPR Policies

Introduction

The General Data protection Regulations (GDPR) were adopted and issued by the EU in May 2016, giving all Member States two year to comply. Its provisions will apply in the UK from 25th May 2018 with a new Data Protection Act 2017, which will incorporate all the provisions of the 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.

Privacy Notice

HC Christensen Dental Practice

We are a Data Controller under the terms of the Data Protection Act 2017 and the requirements of the EU General Data Protection Regulation.

This **Privacy Notice** explains what Personal Data the practice holds, why we hold and process it, who we might share it with, and your rights and freedoms under the Law.

Types of Personal Data

The practice holds personal data in the following categories:

1. Patient clinical and health data and correspondence.
2. Staff employment data.
3. Contractors' data.

Why we process Personal Data (what is the "purpose")

"Process" means we obtain, store, update and archive data.

1. Patient data is held for the purpose of providing patients with appropriate, high quality, safe and effective dental care and treatment.
2. Staff employment data is held in accordance with Employment, Taxation and Pensions law.
3. Contractors' data is held for the purpose of managing their contracts.

What is the Lawful Basis for processing Personal Data?

The Law says we must tell you this:

1. We hold patients' data because it is in our **Legitimate Interest** to do so. Without holding the data we cannot work effectively.
2. We hold staff employment data because it is a **Legal Obligation** for us to do so.
3. We hold contractors' data because it is needed to **Fulfil a Contract** with us.

Who might we share your data with?

We can only share data if it is done securely and it is necessary to do so.

1. Patient data may be shared with other healthcare professionals who need to be involved in your care (for example if we refer you to a specialist or need laboratory work undertaken). Patient data may also be stored for back-up purposes with our computer software suppliers who may also store it securely.
2. Employment data will be shared with government agencies such as HMRC.
3. If patients have opted for the text message reminder/recall service, their phone number and name will be stored by our text message service provider TextMagic.

Your Rights

You have the right to:

1. Be informed about the personal data we hold and why we hold it.
2. Access a copy of your data that we hold by contacting us directly: we will acknowledge your request and supply a response within one month or sooner.
3. Check the information we hold about you is correct and to make corrections if not
4. Have your data erased in certain circumstances.
5. Transfer your data to someone else if you tell us to do so and it is safe and legal to do so.
6. Tell us not to actively process or update your data in certain circumstances.

How long is the Personal Data stored for?

1. We will store patient data for as long as we are providing care, treatment or recalling patients for further care. We will archive (that is, store it without further action) for as long as is required for legal purposes as recommended by the NHS or other trusted experts recommend.
2. We must store employment data for six years after an employee has left.
3. We must store contractors' data for seven years after the contract is ended.

What if you are not happy or wish to raise a concern about our data processing?

You can complain in the first instance to the Christensen Dental Practice and we will do our best to resolve the matter. If this fails, you can complain to the Information Commissioner at www.ico.org.uk/concerns or by calling 0303 123 1113.

Legitimate Interest Assessment

For: Patient, Contractor & Staff Information stored and processed at the Christensen Dental Practice

Part A: Identifying a Legitimate Interest

	Question	Answer
1.	What is the purpose of the processing operation?	For carrying out dental care and treatment of patients
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
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

Part B: The Necessity Test

	Question	Answer
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	Answer
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 patient • Lapsed or cancelled patient • Employee or contractor • Prospective patient • 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 • Periodic • One-off
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	See mitigations in Part D

	reduce or mitigate any underlying privacy risks or harm?	

Part D: Safeguards and Compensating Controls

Safeguards include a range of compensating controls or measures which may be put in place to protect the individual or to reduce any risks or potentially negative impacts of processing. These may have been considered as part of a Privacy Impact Assessment and might include: data minimisation, de-identification, technical and organisational security measures, privacy by design, additional transparency, additional layers of encryption, restricted access, opt-out options.

Part E: Reaching a Decision and Documenting the Outcome

Using the responses above, now document if you believe you are able to rely on Legitimate Interests for the processing operation. Explain, using bullet points why you are, or are not, able to rely on this lawful basis, drawing on the answers provided in this LIA.

Outcome of Assessment:

- 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/we believe the Legitimate Interest threshold is met

Signature: _____

Print Name: _____

Date: _____

Role: _____

Review Date: _____

Data Protection Breach Notification Form

ICO Registration Number (if known): _____

Mandatory details (*)

Section 1: Notification of Breach			
1.*	Date and time incident was discovered		Act as soon as reasonably practical: individual reporting incident to complete
2.*	Date incident occurred if different to above		
3.	Location of incident		e.g. on business premises, at home, in car, etc.
4.	Name of individual reporting incident		
5.	Contact details of individual reporting incident (e-mail & phone)		
6.*	Description of incident and details of lost data		How did the breach occur? Did the data refer to identifiable living individuals?
7.*	Number of data subjects affected if known or approximate		
8.	Brief description of any immediate action taken when discovered		e.g. incorrectly addressed e-mail deleted by recipients; data subject advised, etc.

Section 2: Severity Assessment			
9.	Details of IT system/s, equipment, devices and/or data records involved in the breach		Give as much detail as possible
10.	What information was lost?		Brief description of the category e.g. clinical records, employment data
11.*	What is the nature of the information?		e.g. health data, personal records, financial details
12.	How much data has been lost?		Estimate file sizes, number of records etc. Were entire systems affected?
13.*	Is the information retrievable or replaceable?		Was the data effectively backed up? When? Has it been checked? How old is the back-up?
14.	How many data subjects are involved?		E.g. number of patients, employees affected?
15.	Was the data encrypted?		Details of encryption system used if available
16.*	Is the data sensitive?(GDPR: special under Article 9)		Does data concern health, race or ethnicity, politics or religion
17.*	Do the data subjects include children (<18 years) or vulnerable adults		If so specify approximate numbers or percentages
18.	Does the data include information that could facilitate identity theft?		Does the data include banking details, NI numbers, photocopies of passports or similar
19.*	Does data include information which could cause significant distress or damage?		e.g. details of performance, disciplinary action, or personal lifestyle
20.	Does the information contain security data which might compromise the safety of individuals?		e.g. Access codes, confidential address data, etc.

Section 2: Action Taken (for completion by Data Protection Officer)			
21.*	Name of Data Protection Officer		Include contact details if reporting to ICO
22.	Date and time of receipt of report		
23.	Immediate action taken		e.g. Back-up checked or requested, passwords changed, IT company contacted
24.	Police notified?	• Y/N • Crime number • Badge number/name of Officer/contact • Force name or contact details	e.g. theft of laptop, computer or device, malicious cyber-activity or other criminal action
25.	ICO Notified?	• Y/N • Date and time of notification	Include name of organisation and registration No. if known plus all mandatory details (*), and any previous incidents
26.	Other external stakeholders or regulators notified		e.g. CQC or similar regulator legal advice sought; IT or technical advice sought
27.	Other actions taken by Principals/Data Protection Officer		
28.*	Have affected Data Subjects been notified of loss or theft?	Y/N	Give reason(s) for action taken or proposed
29.	Further Action recommended		

Signature of person reporting breach: _____

Print Name: _____

Date: _____

Signature of Data Protection Officer: _____

Print Name: _____

Date: _____

Note: if the data breach includes information which:

- could cause significant distress or damage to individuals, or
- could compromise the safety of individuals, especially children or vulnerable adults, or
- is of a volume or nature which may cause serious reputational damage

Then consideration should be given to notifying the ICO and also taking advice from expert external sources.

Reports to the Information Commissioner should be made within 72 hours to casework@ico.org.uk with 'DPA Breach Notification form' in the subject field. Further information can be found at: www.ico.org.uk/ - search 'Personal data breaches'.

This record should be kept even if no adverse consequences are anticipated or notifications are required.

Data Audit

Christensen Dental Practice

Business Function		Purpose	Categories of Individuals	Lawful Basis for Processing	Categories of Personal Data	Recipients	Third Countries (outside EEA)
1.	Healthcare provision including diagnosis, care and treatment	Provision of high quality, safe effective and personalised care	• Current patients • Prospective patients • Former patients • Carers/parents	Legitimate interest	• Name • Address/contact details • Date of birth • Dental Plan registration • Health condition • Diagnoses • Care and treatment • Special tests • Third Party Consent Form if required	• Data Subjects, their authorised carers, advisors and trustees • Referral practices • Hospitals • Laboratories • Software companies (patient data) • Dental Plan company • Insurers •	*N/a*
2.	Employment of staff	Lawful employment, taxation, pensions administration Performance management Skills maintenance and enhancement Disciplinary and grievance procedures	• Staff members • Prospective staff members • Former staff members	Fulfilment of contract Legal Duty	• Name • Address/contact details • Date of birth • Health condition (e.g. medical certificates) • National Insurance number	• Data Subjects • Department of Work and Pensions • HM Revenue and Customs • Healthcare Regulators • Software companies (payroll systems)	*N/a*

Business Function		Purpose	Categories of Individuals	Lawful Basis for Processing	Categories of Personal Data	Recipients	Third Countries (outside EEA)
3.	Clinical care (by contracted third parties)	Contractual fulfilment Provision of high quality, safe, effective and personalised care	• Self-employed associate dentists • Self-employed dental care professionals	Fulfilment of Contract	• Name • Address/contact details • Date of birth • Health condition	• Data Subjects • Authorised advisers (e.g. solicitors, accountants)	
4.	Business management - advisory	Contractual fulfilment Lawful, effective and sustainable business management	• Maintenance contractors • Accountants (individuals) • Solicitors (individuals)	Fulfilment of Contract	• Name • Address/contact details	• Data Subjects • Past/prospective owners of the business • HM Customs and Revenue	
5.	Text Message Provider	Reminder, recall and text service provider. Not for marketing purposes	• Current Patients • Contractors • Suppliers	Consent: opt-in	• Name • Mobile phone number	TextMagic	

Audit completed by *[Name]:* _____

Position *[Name]:* _____

Date: _____

Review Date: _____